

Tangent Codes *

AZNIV KASPARIAN

Section of Algebra, Department of Mathematics and Informatics
 Kliment Ohridski University of Sofia
 5 James Bouchier Blvd., Sofia 1164, Bulgaria
email: kasparia@fmi.uni-sofia.bg

EVGENIYA VELIKOVA

Section of Algebra, Department of Mathematics and Informatics
 Kliment Ohridski University of Sofia
 James Bouchier Blvd., Sofia 1164, Bulgaria
email: velikova@fmi.uni-sofia.bg

Abstract

The present article studies the finite Zariski tangent spaces to an affine variety X as linear codes, in order to characterize their typical or exceptional properties by global geometric conditions on X . The discussion concerns the generic minimum distance of a tangent code to X , its lower semi-continuity under a deformation of X , as well as the existence of Zariski tangent spaces to X with exceptional minimum distance. Tangent codes are shown to admit simultaneous decoding. The duals of the tangent codes to X are realized by gradients of polynomials from the ideal of X . We provide constructions of affine varieties with near MDS, cyclic or Hamming tangent codes. Puncturing, shortening and extending finite Zariski tangent spaces are related to the corresponding operations on affine varieties. The $(u|u+v)$ construction of tangent codes is associated with a fibered product of varieties. Explicit constructions realize linear Hamming isometries as differentials of morphisms of affine varieties.

1 Introduction

Codes with additional structure are usually equipped with a priori properties, which facilitate their characterization and decoding. For instance, algebro-geometric Goppa codes allowed Tsfasman, Vlăduț and Zink to improve the asymptotic Gilbert-Varshamov bound on the information rate for a fixed relative minimum distance (cf. [17]). Justesen, Larsen, Elbrønd, Jensen, Havemose, Hoholdt, Skorobogatov, Vlăduț, Krachkovskii, Porter, Duursma, Feng, Rao and others developed efficient algorithms

*2010 *Mathematics Subject Classification*: Primary: 94B27, 14G50; Secondary: 14G17, 11T71
Key words and phrases: Zariski tangent space, minimum distance of a tangent code, simultaneous decoding of tangent codes, gradient codes, operations on codes and affine varieties.

for decoding Goppa codes after obtaining the support of the error of the received word (Pellikaan's [12] is a survey on these results.) Duursma's considerations from [?] imply that the averaged homogeneous weight enumerator of Goppa codes, associated with a complete set of representatives of the linear equivalence classes of divisors of fixed degree is related to the ζ -polynomial of the underlying curve. The realizations of codes by points of a Grassmannian, a determinantal variety or a modification of an arc provide other examples for exploiting "an extra structure" on the objects under study. The interpretation of the finite Zariski tangent spaces to an affine variety X , defined over a finite field \mathbb{F}_q promises to be useful for construction of extremal codes (see Corollary 3) and for simultaneous decoding of a family of codes, after recognizing the error support of the received word (Corollary 8). By grouping linear codes in families we acquire a "dynamic" point of view, which is a natural prerequisite for studying optimization problems. Besides, our families are "integrable" and "geometric", so that various properties of the tangent codes are characterized by global geometric conditions on the corresponding affine variety X (see Proposition 2, Proposition 19, Proposition 20). Explicit constructions of affine varieties realize as finite Zariski tangent spaces near MDS codes (Proposition 12), cyclic codes (Corollary 14), Hamming codes (Proposition 15).

Here is a synopsis of the paper. Section 2 comprises some preliminaries on the Zariski topology and the Zariski tangent spaces $T_a(X, \mathbb{F}_{q^m})$ of an affine variety X .

Our research starts in section 3 by studying the minimum distance $d(T_a(X, \mathbb{F}_{q^m}))$ of $T_a(X, \mathbb{F}_{q^m})$. Proposition 2 (i) from subsection 3.1 establishes that lower bounds on $d(T_a(X, \mathbb{F}_{q^m}))$ hold "almost everywhere" (i.e., on a Zariski open subset of X) if true at some point $a \in X(\mathbb{F}_{q^m}) := X \cap \mathbb{F}_{q^m}$. It provides explicit equations of the exceptional locus $\{b \in X \mid d(T_b(X, \mathbb{F}_{q^m})) < d \text{ for some } m \in \mathbb{N} \text{ with } \mathbb{F}_{q^m}^n \ni b\}$. The deleting $\Pi_\gamma : X \rightarrow \Pi_\gamma(X) \subseteq \overline{\mathbb{F}_q}^{n-|\gamma|}$ of the components, labeled by $\gamma \subseteq \{1, \dots, n\}$ is called the puncturing of X at γ . The presence of a non-finite puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| = d$ coordinates is shown to require all the tangent codes to X to be of minimum distance $\leq d$ (Proposition 2 (ii)). The last part (iii) of Proposition 2 verifies that $d(T_a(X, \mathbb{F}_{q^m})) \geq d + 1$ at "almost all" the points of X whenever all the puncturings $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| = d$ variables are finite and separable (i.e., induce finite separable extensions $\overline{\mathbb{F}_q}(\Pi_\gamma(X)) \subset \overline{\mathbb{F}_q}(X)$ of the corresponding function fields). Corollary 3 from Proposition 2 provides a sufficient condition for a puncturing $\Pi_i : X \rightarrow \Pi_i(X)$ of X at a single variable x_i to preserve the dimension k and the minimum distance d of a generic tangent space. We hope that it could serve as a reasonable base for choice of equations of affine varieties X , whose puncturings realize extremal codes as their Zariski tangent spaces. Corollary 4 from subsection 3.2 constructs an "exotic" embedding of $\overline{\mathbb{F}_q}^k$ in $\overline{\mathbb{F}_q}^n$, whose generic Zariski tangent spaces are $[n, k, d]$ -codes. Any family \mathcal{C} of linear codes $\mathcal{C}(a) \subset \mathbb{F}_q^n$, parameterized by a subset of \mathbb{F}_q^n is interpolated by the union of the Zariski tangent bundles of the irreducible components of an affine variety X , given by explicit equations (cf. Proposition 5 from subsection 3.3).

Proposition 7 from subsection 4.1 proves that the set of the received words $w \in \mathbb{F}_{q^m}^n$ with a $T_a(X, \mathbb{F}_{q^m})$ -error $e \in \mathbb{F}_{q^m}^n$, supported by $i = \{i_1, \dots, i_t\} \subset \{1, \dots, n\}$ coincides

with the Zariski tangent space $T_a(\Pi_i^{-1}(\overline{\Pi_i(X)}), \mathbb{F}_{q^m})$ to the cylinder $\overline{\Pi_i(X)} \simeq \overline{\Pi_i(X)} \times \overline{\mathbb{F}_q}^t$ over the Zariski closure $\overline{\Pi_i(X)}$ of the puncturing $\Pi_i(X)$ of X at i . That reduces the calculation of the error e to solving a linear system of $t < n$ variables. Moreover, Corollary 8 provides an algorithm for simultaneous decoding of finite Zariski tangent spaces to X of minimum distance $\geq 2t+1$. The procedure supplies several polynomial matrices by the means of Groebner bases computations. For an arbitrary received word $w \in \mathbb{F}_{q^m}^n$ with a $T_a(X, \mathbb{F}_{q^m})$ -error $e \in \mathbb{F}_{q^m}^n$ of weight $\leq t$, one evaluates a part of the constructed polynomial matrices at a and calculates their products with the transposed w^t of the received word w , in order to recognize a t -tuple i , containing the support of e and to obtain the components of e , labeled by i . Subsection 4.2 discusses the dependence of the generic minimum distance of a tangent code on the equations of X . More precisely, Proposition 9 shows that a generic deformation of X through a fixed point $a \in X$ with tangent code $T_a(X, \mathbb{F}_{q^m})$ of minimum distance d has generic minimum distance $\geq d$ of the finite Zariski tangent spaces. The last subsection 4.3 of section 4 is devoted to the dual codes $T_a(X, \mathbb{F}_{q^m})^\perp$ of the finite Zariski tangent spaces. By Lemma 10, $T_a(X, \mathbb{F}_{q^m})^\perp$ consists of the gradients of the polynomials from $I(X, \mathbb{F}_{q^m})$ at a . Let $\beta \subset \{1, \dots, n\}$ be a d -tuple of indices with complement $\neg\beta := \{1, \dots, n\} \setminus \beta$. Proposition 11 establishes that if "almost all" the points of $\overline{\mathbb{F}_q}^d$ are from the image of the puncturing $\Pi_{\neg\beta} : X \rightarrow \overline{\mathbb{F}_q}^d$ and the absolute ideal $I(X, \overline{\mathbb{F}_q})$ of X contains a non-zero polynomial in $x_\beta = \{x_{\beta_1}, \dots, x_{\beta_d}\}$ then the generic minimum distance of a gradient code to X is $\leq d$.

Section 5 discusses tangent codes of special type. Proposition 12 from subsection 5.1 establishes that if X admits a non-finite puncturing $\Pi_\alpha : X \rightarrow \Pi_\alpha(X)$ at $|\alpha| = n-k$ variables and at least one tangent code to X at a smooth point is a near MDS code then "almost all" the finite Zariski tangent spaces to X are near MDS. In a contrast, the locus of the cyclic tangent codes is shown to be exceptional in subsection 5.2. Corollary 14 (i) provides the equations of this locus in the set X^{smooth} of the smooth points of X . Let p be a prime integer, relatively prime to $n \in \mathbb{N}$ and \mathbb{F}_{p^m} be the splitting field of $t^n - 1 \in \mathbb{F}_p[t]$ over \mathbb{F}_p . We say that $T_a(X, \mathbb{F}_{p^s})$ with $a \in X(\mathbb{F}_{p^s})$ is a cyclic tangent code if there is a cyclic code $C \subset \mathbb{F}_{p^m}^n$ with $T_a(X, \mathbb{F}_{p^s}) \otimes_{\mathbb{F}_{p^s}} \mathbb{F}_{p^{ms}} = C \otimes_{\mathbb{F}_{p^m}} \mathbb{F}_{p^{ms}}$. All cyclic codes of length n over $\overline{\mathbb{F}_p}$ are realized as finite Zariski tangent spaces to X if for any cyclic code $C \subset \mathbb{F}_{p^m}^n$ there exists a point $a \in X(\mathbb{F}_{p^s})$, such that $C \otimes_{\mathbb{F}_{p^m}} \mathbb{F}_{p^{ms}} = T_a(X, \mathbb{F}_{p^s}) \otimes_{\mathbb{F}_{p^s}} \mathbb{F}_{p^{ms}}$. Explicit constructions provide affine varieties, whose finite Zariski tangent spaces realize all the cyclic codes of length n over $\overline{\mathbb{F}_p}$. Among them, there is an example, whose all tangent codes are cyclic (cf. Corollary 14 (ii)). For any natural number M we provide an affine variety, whose finite Zariski tangent spaces realize all cyclic codes of length n over $\overline{\mathbb{F}_p}$ and contain at least M non-cyclic tangent codes (Corollary 14 (iii)). For an arbitrary finite field \mathbb{F}_q and an arbitrary natural number r , let us put $n := \frac{q^r-1}{q-1}$. Proposition 15 from subsection 5.3 constructs an exotic embedding of $\overline{\mathbb{F}_q}^{n-r}$ in $\overline{\mathbb{F}_q}^n$, which has $q(q-1)^{n-r-1}$ Hamming tangent codes in the case of an odd characteristic $\text{char}\mathbb{F}_q$ or q^{n-r} Hamming tangent codes for $\text{char}\mathbb{F}_q = 2$.

Section 6 draws parallels between operations on tangent codes and operations on the corresponding affine varieties. If the tangent codes to X are of generic minimum

distance d and the differentials of a puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| < d$ coordinates are generically surjective then the generic tangent vectors to $\Pi_\gamma(X)$ of minimum weight $d - |\gamma|$ are shown in Corollary 18 to be the puncturings of the generic tangent vectors to X of weight d , containing γ in its support. For an appropriate index set γ of cardinality $|\gamma| \leq \dim X$, Proposition 19 establishes the coincidence of the shortenings of the tangent codes to X on γ with the tangent codes to the shortening $X \cap V(x_i \mid i \in \gamma)$ of X on γ . Similarly, the puncturings of the gradient codes to X at γ are exactly the gradient codes to the shortening $X \cap V(x_i \mid i \in \gamma)$ of X on γ . Another set of assumptions guarantee the coincidence of the shortenings of the gradient codes to X on γ with the gradient codes to the puncturing $\Pi_\gamma(X)$ of X at γ . The extension of a tangent code to X is proved to be a Zariski tangent space to the extension of X in subsection 6.3. The direct sum of finite Zariski tangent spaces to affine varieties X, Y turns to be a Zariski tangent space to the direct product $X \times Y$. The $(u \mid u + v)$ construction of tangent codes is realized as a Zariski tangent space to a fibered product of appropriate affine varieties.

The final, seventh section constructs a morphism $\overline{\mathbb{F}}_q^n \rightarrow \overline{\mathbb{F}}_q^n$, whose differentials are linear Hamming isometries of "almost all" Zariski tangent spaces to "almost all" affine varieties $X \subset \overline{\mathbb{F}}_q^n$ (Proposition 21). An arbitrary family of linear Hamming isometries $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, parameterized by \mathbb{F}_q^n is interpolated by differentials of an explicit morphism $\overline{\mathbb{F}}_q^n \rightarrow \overline{\mathbb{F}}_q^n$.

We conclude with an immediate consequence of results of Duursma, which relates the ζ -polynomials of an appropriate family of Goppa codes with the ζ -polynomial of the underlying curve. This is one more evidence that the algebraic geometry provides a reasonable grouping of linear codes in families.

Acknowledgements: The authors are grateful to the referee of Finite Fields and their Applications for the useful remarks and suggestions. The research is partially supported by Contract 015/2014 and Contract 144/2015 with the Scientific Foundation of Kliment Ohridski University of Sofia.

2 Algebraic geometry preliminaries

Let $\overline{\mathbb{F}}_q = \cup_{m=1}^{\infty} \mathbb{F}_{q^m}$ be the algebraic closure of the finite field \mathbb{F}_q with q elements and $\overline{\mathbb{F}}_q^n$ be the n -dimensional affine space over $\overline{\mathbb{F}}_q$. An affine variety $X \subset \overline{\mathbb{F}}_q^n$ is the common zero set

$$X = V(f_1, \dots, f_m) = \{a \in \overline{\mathbb{F}}_q^n \mid f_1(a) = \dots = f_m(a) = 0\}$$

of polynomials $f_1, \dots, f_m \in \overline{\mathbb{F}}_q[x_1, \dots, x_n]$. We say that $X \subset \overline{\mathbb{F}}_q^n$ is defined over \mathbb{F}_q and denote $X/\mathbb{F}_q \subset \overline{\mathbb{F}}_q^n$ if the absolute ideal

$$I(X, \overline{\mathbb{F}}_q) := \{f \in \overline{\mathbb{F}}_q[x_1, \dots, x_n] \mid f(a) = 0, \forall a \in X\}$$

of X is generated by polynomials $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ with coefficients from \mathbb{F}_q .

The affine subvarieties of X form a family of closed subsets. The corresponding topology is referred to as the Zariski topology on X . The Zariski closure \overline{M} of a subset

$M \subseteq X$ is defined as the intersection of the Zariski closed subsets Z of X , containing M . It is easy to observe that $\overline{M} = VI(M, \overline{\mathbb{F}_q})$ is the affine variety of the absolute ideal $I(M, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ of M . A subset $M \subseteq X$ is Zariski dense if its Zariski closure $\overline{M} = X$ coincides with X . A property $\mathcal{P}(a)$, depending on a point $a \in \overline{\mathbb{F}_q}^n$ holds at a generic point of an affine variety $X \subset \overline{\mathbb{F}_q}^n$ if there is a Zariski dense subset $M \subseteq X$, such that $\mathcal{P}(a)$ is true for all $a \in M$.

An affine variety $X \subset \overline{\mathbb{F}_q}^n$ is irreducible if any decomposition $X = Z_1 \cup Z_2$ into a union of Zariski closed subsets $Z_j \subseteq X$ has $Z_1 = X$ or $Z_2 = X$. This holds exactly when the absolute ideal $I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ of X is prime, i.e. $fg \in I(X, \overline{\mathbb{F}_q})$ for $f, g \in \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ requires $f \in I(X, \overline{\mathbb{F}_q})$ or $g \in I(X, \overline{\mathbb{F}_q})$. A prominent property of the irreducible affine varieties X is the Zariski density of an arbitrary non-empty Zariski open subset $U \subseteq X$. This is equivalent to $U \cap W \neq \emptyset$ for any non-empty Zariski open subsets $U \subseteq X$ and $W \subseteq X$.

For an arbitrary irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, defined over \mathbb{F}_q and an arbitrary constant field $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}_q}$, the affine coordinate ring

$$F[X] := F[x_1, \dots, x_n]/I(X, F)$$

of X over F is an integral domain. The fraction field

$$F(X) := \left\{ \frac{\varphi_1}{\varphi_2} \mid \varphi_1, \varphi_2 \in F[X], \varphi_2 \neq 0 \in F[X] \right\}$$

of $F[X]$ is called the functional field of X over F . The points $a \in X$ correspond to the maximal ideals $I(a, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$, containing $I(X, \overline{\mathbb{F}_q})$. For any F -rational point $a \in X(F) := X \cap F^n$ the localization

$$\mathcal{O}_a(X, F) := \left\{ \frac{\varphi_1}{\varphi_2} \mid \varphi_1, \varphi_2 \in F[X], \varphi_2(a) \neq 0 \right\}$$

of $F[X]$ at $F[X] \setminus (I(a, F)/I(X, F))$ is the local ring of a in X over F . An F -linear derivation $D_a : \mathcal{O}_a(X, F) \rightarrow F$ at $a \in X(F)$ is an F -linear map, subject to Leibnitz-Newton rule $D_a(\psi_1\psi_2) = D_a(\psi_1)\psi_2(a) + \psi_1(a)D_a(\psi_2)$ for $\forall \psi_1, \psi_2 \in \mathcal{O}_a(X, F)$. The F -linear space

$$T_a(X, F) := \text{Der}_a(\mathcal{O}_a(X, F), F)$$

of the F -linear derivations $D_a : \mathcal{O}_a(X, F) \rightarrow F$ at $a \in X(F)$ is called the Zariski tangent space to X at a over F .

In order to derive a coordinate description of $T_a(X, F)$, note that any F -linear derivation $D_a : \mathcal{O}_a(X, F) \rightarrow F$ at $a \in X(F)$ restricts to an F -linear derivation $D_a : F[X] \rightarrow F$ at a . According to

$$D_a(\varphi_1) = D_a\left(\frac{\varphi_1}{\varphi_2}\right)\varphi_2(a) + \frac{\varphi_1(a)}{\varphi_2(a)}D_a(\varphi_2) \quad \text{for } \forall \varphi_1, \varphi_2 \in F[X] \quad \text{with } \varphi_2(a) \neq 0,$$

any F -linear derivation $D_a : F[X] \rightarrow F$ at $a \in X(F)$ has unique extension to an F -linear derivation $D_a : \mathcal{O}_a(X, F) \rightarrow F$ at a . In such a way, there arises an F -linear isomorphism

$$T_a(X, F) \simeq \text{Der}_a(F[X], F).$$

Any F -linear derivation $D_a : F[X] \rightarrow F$ of the affine ring $F[X]$ of X at $a \in X(F)$ lifts to an F -linear derivation $D_a : F[x_1, \dots, x_n] \rightarrow F$ of the polynomial ring at a , vanishing on the ideal $I(X, F)$ of X over F . If $I(X, F) = \langle f_1, \dots, f_m \rangle_F \triangleleft F[x_1, \dots, x_n]$ is generated by $f_1, \dots, f_m \in F[x_1, \dots, x_n]$ then for arbitrary $g_1, \dots, g_m \in F[x_1, \dots, x_n]$ one has

$$D_a \left(\sum_{i=1}^m f_i g_i \right) = \sum_{i=1}^m D_a(f_i) g_i(a)$$

and the Zariski tangent space

$$T_a(X, F) \simeq \{D_a \in \text{Der}_a(F[x_1, \dots, x_n], F) \mid D_a(f_1) = \dots = D_a(f_m) = 0\}$$

to X at a consists of the derivations $D_a : F[x_1, \dots, x_n] \rightarrow F$ at a , vanishing on f_1, \dots, f_m . In such a way, the coordinate description of $T_a(X, F)$ reduces to the coordinate description of

$$\text{Der}_a(F[x_1, \dots, x_n], F) = \text{Der}_a(F[\overline{\mathbb{F}}_q^n], F) = T_a(\overline{\mathbb{F}}_q^n, F).$$

In order to endow $T_a(\overline{\mathbb{F}}_q^n, F)$ with a basis over F , let us note that the polynomial ring

$$F[x_1, \dots, x_n] = F[x_1 - a_1, \dots, x_n - a_n] = \bigoplus_{i=0}^{\infty} F[x_1 - a_1, \dots, x_n - a_n]^{(i)}$$

has a natural grading by the F -linear spaces $F[x_1 - a_1, \dots, x_n - a_n]^{(i)}$ of the homogeneous polynomials on $x_1 - a_1, \dots, x_n - a_n$ of degree $i \geq 0$. An arbitrary F -linear derivation $D_a : F[x_1, \dots, x_n] \rightarrow F$ at $a \in F^n$ vanishes on $F[x_1 - a_1, \dots, x_n - a_n]^{(0)} = F$ and on the homogeneous polynomials $F[x_1 - a_1, \dots, x_n - a_n]^{(i)}$ of degree $i \geq 2$. Thus, D_a is uniquely determined by its restriction to the n -dimensional space

$$F[x_1 - a_1, \dots, x_n - a_n]^{(1)} = \text{Span}_F(x_1 - a_1, \dots, x_n - a_n)$$

over F . That enables to identify the Zariski tangent space

$$T_a(\overline{\mathbb{F}}_q^n, F) \simeq \text{Der}_a(F[x_1, \dots, x_n], F) \simeq \text{Hom}_F(F[x_1 - a_1, \dots, x_n - a_n]^{(1)}, F)$$

to $\overline{\mathbb{F}}_q^n$ at a with the space of the F -linear functionals on $F[x_1 - a_1, \dots, x_n - a_n]^{(1)}$. Note that $x_1 - a_1, \dots, x_n - a_n$ is a basis of $F[x_1 - a_1, \dots, x_n - a_n]^{(1)}$ over F and denote by $\left(\frac{\partial}{\partial x_1}\right)_a, \dots, \left(\frac{\partial}{\partial x_n}\right)_a$ its dual basis. In other words, $\left(\frac{\partial}{\partial x_j}\right)_a \in T_a(\overline{\mathbb{F}}_q^n, F)$ are the uniquely determined F -linear functionals on $F[x_1 - a_1, \dots, x_n - a_n]^{(1)}$ with

$$\left(\frac{\partial}{\partial x_j}\right)_a (x_i - a_i) = \delta_{ij} = \begin{cases} 1 & \text{for } 1 \leq i = j \leq n, \\ 0 & \text{for } 1 \leq i \neq j \leq n. \end{cases}$$

As a result, the Zariski tangent space to X at $a \in X(F)$ over F can be described as

$$T_a(X, F) = \left\{ v = \sum_{j=1}^n v_j \left(\frac{\partial}{\partial x_j}\right)_a \mid \sum_{j=1}^n v_j \frac{\partial f_i}{\partial x_j}(a) = 0, \quad 1 \leq i \leq m \right\}$$

for any generating set f_1, \dots, f_m of $I(X, F) = \langle f_1, \dots, f_m \rangle_F$. If

$$\frac{\partial f}{\partial x} = \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)} = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}$$

is the Jacobian matrix of f_1, \dots, f_m and $F = \mathbb{F}_{q^s}$ is a finite field then $T_a(X, \mathbb{F}_{q^s}) \subset \mathbb{F}_{q^s}^n$ is the \mathbb{F}_{q^s} -linear code with parity check matrix $\frac{\partial f}{\partial x}(a) \in M_{m \times n}(\mathbb{F}_{q^s})$.

Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety with $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$, $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$. For an arbitrary point $a = (a_1, \dots, a_n) \in X$, let us denote by $\delta(a)$ the minimal natural number, for which $a \in X(\mathbb{F}_{q^{\delta(a)}}) := X \cap \mathbb{F}_{q^{\delta(a)}}^n$ is an $\mathbb{F}_{q^{\delta(a)}}$ -rational point of X . We say that $\mathbb{F}_{q^{\delta(a)}}$ is the definition field of a over \mathbb{F}_q . If $\mathbb{F}_{q^{\delta(a_i)}}$ are the definition fields of $a_i \in \overline{\mathbb{F}_q}$ over \mathbb{F}_q then $\delta(a)$ is the least common multiple of $\delta(a_1), \dots, \delta(a_n)$. Note that $a \in X(\mathbb{F}_{q^m})$ is an \mathbb{F}_{q^m} -rational point if and only if $\delta(a)$ divides m . For all $l \in \mathbb{N}$ the Zariski tangent spaces $T_a(X, \mathbb{F}_{q^{l\delta(a)}})$ have one and a same parity check matrix

$$\frac{\partial f}{\partial x}(a) := \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(a) \in M_{m \times n}(\mathbb{F}_{q^{\delta(a)}})$$

and are uniquely determined by $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ as the tensor products

$$T_a(X, \mathbb{F}_{q^{l\delta(a)}}) = T_a(X, \mathbb{F}_{q^{\delta(a)}}) \otimes_{\mathbb{F}_{q^{\delta(a)}}} \mathbb{F}^{l\delta(a)}.$$

In particular, $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ and $T_a(X, \mathbb{F}_{q^{l\delta(a)}})$ have equal dimension $n - \text{rk}_{\mathbb{F}_{q^{\delta(a)}}} \frac{\partial f}{\partial x}(a)$ over $\mathbb{F}_{q^{\delta(a)}}$, respectively, over $\mathbb{F}_{q^{l\delta(a)}}$. The minimum distances of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ and $T_a(X, \mathbb{F}_{q^{l\delta(a)}})$ coincide, as far as they equal the minimal natural number d for which $\frac{\partial f}{\partial x}(a)$ has d linearly dependent columns. From now on, we write $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}})$ for the dimension of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ over $\mathbb{F}_{q^{\delta(a)}}$.

Let $X = X_1 \cup \dots \cup X_s$ be a reducible affine variety and $a \in X_{i_1} \cap \dots \cap X_{i_r}$ with $1 \leq i_1 < \dots < i_r \leq s$ be a common point of $r \geq 2$ irreducible components X_{i_j} of X . In general, X_{i_j} have different Zariski tangent spaces at a and the union $T_a(X_{i_1}, \mathbb{F}_{q^{\delta(a)}}) \cup \dots \cup T_a(X_{i_r}, \mathbb{F}_{q^{\delta(a)}})$ is not an $\mathbb{F}_{q^{\delta(a)}}$ -linear subspace of $\mathbb{F}_{q^{\delta(a)}}^n$. That is why we define the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ to a reducible variety $X \subset \overline{\mathbb{F}_q}^n$ at a point $a \in X$ as the $\mathbb{F}_{q^{\delta(a)}}$ -linear code of length n with parity check matrix

$$\frac{\partial f}{\partial x}(a) = \frac{\partial(f_1, \dots, f_m)}{\partial(x_1, \dots, x_n)}(a) \in M_{m \times n}(\mathbb{F}_{q^{\delta(a)}}),$$

for some generators $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ of the absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ of X .

For an arbitrary finite set S and an arbitrary natural number $t \leq |S|$ let us denote by $\Sigma_t(S)$ the set of the t -tuples with entries from S . In the case of $S = \{1, \dots, n\}$, we write $\Sigma_t(1, \dots, n)$ instead of $\Sigma_t(\{1, \dots, n\})$.

For a systematic study of the Zariski tangent spaces to an affine variety see [16], [2], [11], [14] or [7].

3 Minimum distance of a tangent code

3.1 Typical minimum distance of a tangent code

The minimum distance of a linear code $C \subset \mathbb{F}_q^n$ is related to the kernels of the puncturings of C . Note that the puncturing

$$\Pi_\gamma : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow \Pi_\gamma T_a(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq \mathbb{F}_{q^{\delta(a)}}^{n-|\gamma|}$$

of a finite Zariski tangent space to X coincides with the differential

$$\Pi_\gamma = (d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

of the puncturing

$$\Pi_\gamma : X \longrightarrow \Pi_\gamma(X)$$

of the corresponding irreducible affine variety X . That allows to study the minimum distance of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ by the global properties of $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$.

In order to formulate precisely, let us recall that a finite morphism $\varphi : X \rightarrow \varphi(X)$ is called separable if the finite extension $\overline{\mathbb{F}_q}(\varphi(X)) \subseteq \overline{\mathbb{F}_q}(X)$ of the corresponding function fields is separable. This means that the minimal polynomial $g_\xi(t) \in \overline{\mathbb{F}_q}(\varphi(X))[t]$ of an arbitrary element $\xi \in \overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\varphi(X))$ has no multiple roots.

A morphism $\varphi : X \rightarrow \varphi(X)$ is etale at some point $a \in X$, if the differential $(d\varphi)_a : T_a(X, \overline{\mathbb{F}_q}) \rightarrow T_{\varphi(a)}(\varphi(X), \overline{\mathbb{F}_q})$ of φ at a is an $\overline{\mathbb{F}_q}$ -linear embedding. Let us denote by $\text{Etale}(\varphi)$ the set of the points $a \in X$, at which the morphism $\varphi : X \rightarrow \varphi(X)$ is etale.

Lemma 1. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over \mathbb{F}_q and $\Pi_\gamma : X \rightarrow \Pi_\gamma(X) \subseteq \overline{\mathbb{F}_q}^{n-|\gamma|}$ be a puncturing at a subset $\gamma \subseteq \{1, \dots, n\}$.*

(i) The puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is etale at $a \in X$ if and only if the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ does not contain a non-zero word $v(a)$ with support $\text{Supp}(v(a)) \subseteq \gamma$.

(ii) If the set $\text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}}) \neq \emptyset$ is non-empty then the puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is a finite morphism, $\text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}}) \subseteq X^{\text{smooth}}$ and the differentials

$$(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

are surjective at all the points $a \in \text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$.

(iii) If the puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is a finite separable morphism then $\text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ is a Zariski dense subset of X .

Proof. (i) The kernel of the differential $(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \rightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ consists of the tangent vectors $v(a) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ with support $\text{Supp}(v(a)) \subseteq \gamma$.

(ii) Note that $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \geq \dim X = k$ at any point $a \in X$. If $a \in \text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ then $(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \rightarrow T_{\Pi_\gamma(a)}(X, \mathbb{F}_{q^{\delta(a)}})$ is injective and $\dim T_{\Pi_\gamma(a)}(X, \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X)$. Combining with $\dim \Pi_\gamma(X) \leq \dim X$,

one obtains

$$\dim X \leq \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim(d\Pi_\gamma)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) \leq \dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X) \leq \dim X.$$

Therefore $(d\Pi_\gamma)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$, $\dim X = \dim T_a(X, \overline{\mathbb{F}_q})$ and the dimensions $\dim \Pi_\gamma(X) = \dim X$ coincide. In other words, the differential $(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \rightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$ is surjective, $a \in X^{\text{smooth}}$ is a smooth point and $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is a finite morphism.

(iii) In order to show that $\text{Etale}(\Pi_\gamma)$ contains a non-empty Zariski open subset of X , let us consider the minimal polynomials

$$g_i(t, \overline{x_{-\gamma}}) = \sum_{s=0}^{N_i} \frac{\varphi_{i,s}(\overline{x_{-\gamma}})}{\psi_{i,s}(\overline{x_{-\gamma}})} t^s \in \overline{\mathbb{F}_q}(\overline{x_{-\gamma}})[t]$$

of $\overline{x_i} = x_i + I(X, \overline{\mathbb{F}_q}) \in \overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\Pi_\gamma(X)) = \overline{\mathbb{F}_q}(\overline{x_{-\gamma}})$ with $\varphi_{i,s}(\overline{x_{-\gamma}}), \psi_{i,s}(\overline{x_{-\gamma}}) \in \overline{\mathbb{F}_q}[\overline{x_{-\gamma}}] := \overline{\mathbb{F}_q}[x_{-\gamma}]/I(X, \overline{\mathbb{F}_q})$. Denote by $\psi_i(x_{-\gamma}) \in \overline{\mathbb{F}_q}[x_{-\gamma}]$ the least common multiple of the polynomials $\psi_{i,s}(x_{-\gamma}) \in \overline{\mathbb{F}_q}[x_{-\gamma}]$, $0 \leq s \leq N_i$. The polynomial $\psi_i(x_{-\gamma})$ is well defined up to a factor from $\overline{\mathbb{F}_q}[x_{-\gamma}]^* = \overline{\mathbb{F}_q}^*$. The product

$$f_i(x_i, x_{-\gamma}) := \psi_i(x_{-\gamma}) g_i(x_i, x_{-\gamma}) \in \overline{\mathbb{F}_q}[x_i, x_{-\gamma}] \cap I(X, \overline{\mathbb{F}_q})$$

is a polynomial of minimal degree with respect to x_i from $I(X, \overline{\mathbb{F}_q})$. We claim that the Zariski open subset

$$W := X \setminus V \left(\prod_{i \in \gamma} \frac{\partial f_i}{\partial x_i} \right)$$

is non-empty and contained in $\text{Etale}(\Pi_\gamma)$. More precisely, $f_{\gamma_1}, \dots, f_{\gamma_d} \in I(X, \overline{\mathbb{F}_q})$ for $\gamma = \{\gamma_1, \dots, \gamma_d\}$ implies that $T_a(X, \overline{\mathbb{F}_q})$ is contained in the solution set \mathcal{S} of the homogeneous linear system with coefficient matrix $H_\gamma = \frac{\partial f_\gamma}{\partial x}(a)$. If we arrange the variables $x = \{x_1, \dots, x_n\}$ in two groups - x_γ and $x_{-\gamma}$, then $\frac{\partial f_\gamma}{\partial x_\gamma}(a)$ is a diagonal matrix with non-zero entries for any $a \in W$. As a result, the components $v_\gamma = v_\gamma(v_{-\gamma})$ of $v = (v_\gamma, v_{-\gamma}) \in \mathcal{S}$, labeled by γ can be expressed as homogeneous linear functions of $v_{-\gamma}$ and the puncturing $\Pi_\gamma : \mathcal{S} \rightarrow \Pi_\gamma(\mathcal{S})$ is injective. Then the restriction $\Pi_\gamma = (d\Pi_\gamma)_a : T_a(X, \overline{\mathbb{F}_q}) \rightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \overline{\mathbb{F}_q})$ of $\Pi_\gamma|_{\mathcal{S}}$ is injective and $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is etale at any point $a \in W$. That justifies $\text{Etale}(\Pi_\gamma) \supseteq W$.

The assumption $W = \emptyset$ implies that

$$X \subseteq V \left(\prod_{i \in \gamma} \frac{\partial f_i}{\partial x_i} \right).$$

As a result, $\prod_{i \in \gamma} \frac{\partial f_i}{\partial x_i} \in I(X, \overline{\mathbb{F}_q})$. The absolute ideal $I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ of the irreducible affine variety $X \subseteq \overline{\mathbb{F}_q}^n$ is prime and there follows $\frac{\partial f_i}{\partial x_i} \in I(X, \overline{\mathbb{F}_q})$ for some

$i \in \gamma$. Since $f_i \in I(X, \overline{\mathbb{F}_q}) \setminus \{0\}$ is of minimum degree with respect to x_i , one concludes that $\frac{\partial f_i}{\partial x_i} \equiv 0 \in \overline{\mathbb{F}_q}[x_1, \dots, x_n]$. However, $\frac{\partial f_i}{\partial t}(t, x_{-\gamma}) = \psi_i(x_{-\gamma}) \frac{\partial g_i}{\partial t}(t, x_{-\gamma})$ implies that $\frac{\partial g_i}{\partial t}(t, x_{-\gamma}) \equiv 0$ and $g_i(t, \overline{x_{-\gamma}}) \in \overline{\mathbb{F}_q}(\overline{x_{-\gamma}})[t]$ has a multiple root. That contradicts the separability of the finite extension $\overline{\mathbb{F}_q}(\overline{x_{-\gamma}}) \subseteq \overline{\mathbb{F}_q}(X)$ and proves that $W \neq \emptyset$.

The non-empty Zariski open subset $\Pi_\gamma(X)^{\text{smooth}} \subseteq \Pi_\gamma(X)$ pulls back to a non-empty Zariski open subset $W_\gamma := \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}}) \subseteq X$. The intersection $W \cap W_\gamma$ is a non-empty Zariski open and, therefore, Zariski dense subset of the irreducible affine variety X . Thus, the Zariski closures $X \supseteq \overline{\text{Etale}(\Pi_\gamma) \cap W_\gamma} \supseteq \overline{W \cap W_\gamma} = X$ coincide with X and $\text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ is Zariski dense in X . \square

Note that Lemma 1 (ii) establishes a sort of a generalization of the Implicit Function Theorem, according to which any puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ with an injective differential at some point $a \in \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ is a finite morphism.

For an arbitrary irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, defined over \mathbb{F}_q , let us denote by

$$X^{(\leq d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq d\}$$

the set of the points $a \in X$, at which the finite Zariski tangent spaces are of minimum distance $\leq d$. Similarly, put

$$X^{(d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) = d\} \quad \text{and}$$

$$X^{(\geq d)} := \{a \in X \mid d(X, \mathbb{F}_{q^{\delta(a)}}) \geq d\}.$$

The next proposition establishes that if an irreducible affine variety X admits a tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ of minimum distance $\geq d$ then "almost all" finite Zariski tangent spaces to X are of minimum distance $\geq d$. If there is a non-finite puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| = d$ variables, we show that all the tangent codes to X are of minimum distance $\leq d$. When all the puncturings $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| = d$ variables are finite and separable, the minimum distance of a finite Zariski tangent space to X is bounded below by $d + 1$ at "almost all" the points of X .

Proposition 2. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety of dimension $k \in \mathbb{N}$ with $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ for some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$.*

(i) *For an arbitrary natural number $d \leq n - k + 1$ the locus*

$$X^{(\leq d)} = V \left(\prod_{i \in \Sigma_d(1, \dots, n)} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \mid \forall \varphi : \Sigma_d(1, \dots, n) \rightarrow \Sigma_d(1, \dots, m) \right)$$

is a Zariski closed subset of X and $X^{(\leq 1)} \subseteq X^{(\leq 2)} \subseteq \dots \subseteq X^{(\leq n-k+1)} = X$.

(ii) *If there is a non-finite puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at $|\gamma| = d$ coordinates then $X = X^{(\leq d)}$. Moreover, in the case of $X^{(d)} \neq \emptyset$ the locus $X^{(d)} = X^{(\geq d)}$ is a Zariski dense, Zariski open subset of X .*

(iii) *If for any $\gamma \in \Sigma_d(1, \dots, n)$ the puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is finite and separable then the subset $X^{(\geq d+1)} \subseteq X$ is Zariski dense.*

Proof. (i) For an arbitrary natural number $d \leq n - k$, observe that $a \in X^{(>d)} = X^{(\geq d+1)}$ exactly when any d -tuple of columns of $\frac{\partial f}{\partial x}(a)$ is linearly independent. That amounts to $\text{rk} \frac{\partial f}{\partial x_i}(a) = \text{rk} \frac{\partial(f_1, \dots, f_m)}{\partial(x_{i_1}, \dots, x_{i_d})}(a) = d$ for all $i \in \Sigma_d(1, \dots, n)$. By $k = \dim X \geq n - m$ there follows $m \geq n - k \geq d$ and $\text{rk} \frac{\partial f}{\partial x_i}(a) = d$ is equivalent to $\det \frac{\partial f_\gamma}{\partial x_i}(a) \neq 0$ for some $\gamma \in \Sigma_d(1, \dots, m)$. Thus,

$$\begin{aligned} X^{(\geq d+1)} &= \cap_{i \in \Sigma_d(1, \dots, n)} \left[\cup_{\gamma \in \Sigma_d(1, \dots, m)} \left(X \setminus V \left(\det \frac{\partial f_\gamma}{\partial x_i} \right) \right) \right] = \\ &= \cap_{i \in \Sigma_d(1, \dots, n)} \left[X \setminus V \left(\det \frac{\partial f_\gamma}{\partial x_i} \mid \gamma \in \Sigma_d(1, \dots, m) \right) \right] = \\ &= X \setminus \cup_{i \in \Sigma_d(1, \dots, n)} V \left(\det \frac{\partial f_\gamma}{\partial x_i} \mid \gamma \in \Sigma_d(1, \dots, m) \right) = \\ &= X \setminus V \left(\prod_{i \in \Sigma_d(1, \dots, n)} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \mid \varphi : \Sigma_d(1, \dots, n) \rightarrow \Sigma_d(1, \dots, m) \right). \end{aligned} \quad (1)$$

The last equality follows from $\cup_{i \in \Sigma_d(1, \dots, n)} V(S_i) = V \left(\prod_{i \in \Sigma_d(1, \dots, n)} S_i \right)$ for

$$\prod_{i \in \Sigma_d(1, \dots, n)} S_i := \left\{ \prod_{i \in \Sigma_d(1, \dots, n)} g_i \mid g_i \in S_i \right\}, \quad S_i := \left\{ \det \frac{\partial f_\gamma}{\partial x_i} \mid \gamma \in \Sigma_d(1, \dots, m) \right\}.$$

The complement

$$\begin{aligned} X^{(\leq d)} &= X \setminus X^{(\geq d+1)} = \\ &= X \cap V \left(\prod_{i \in \Sigma_d(1, \dots, n)} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \mid \varphi : \Sigma_d(1, \dots, n) \rightarrow \Sigma_d(1, \dots, m) \right) \end{aligned}$$

is a Zariski closed subset of X .

For an arbitrary point $a \in X$, note that $\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \geq \dim X = k$. Singleton bound on the minimum distance requires

$$d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \leq n + 1 - \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \leq n + 1 - k.$$

Thus, $X = X^{(\leq n-k+1)}$ is also a Zariski closed subset of X .

(ii) Note that the non-empty Zariski open subset $\Pi_\gamma(X)^{\text{smooth}}$ of $\Pi_\gamma(X)$ pulls back to a non-empty Zariski open subset $W_\gamma := \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ of X . We claim that at any $a \in W_\gamma$ the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ contains a non-zero word, supported by γ . To this end, it suffices to establish that the differential

$$(d\Pi_\gamma)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}})$$

of Π_γ at a is non-injective. Assume the opposite, i.e., that $\ker(d\Pi_\gamma)_a = 0$. Then

$$k \leq \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \leq \dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X).$$

The morphism $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is not finite, so that $\dim \Pi_\gamma(X) < \dim X = k$. That leads to a contradiction and implies that $\ker(d\Pi_\gamma)_a \neq 0$ for $\forall a \in W_\gamma$. As a result, $W_\gamma \subseteq X^{(\leq d)}$. According to (i), $X^{(\leq d)}$ is a Zariski closed subset of X , so that the inclusion $X = \overline{W_\gamma} \subseteq \overline{X^{(\leq d)}} = X^{(\leq d)}$ of the corresponding Zariski closures is tantamount to $X = X^{(\leq d)}$. Now, $X^{(d)} = X^{(\leq d)} \cap X^{(\geq d)} = X \cap X^{(\geq d)} = X^{(\geq d)}$ is a Zariski open subset of X , whereas Zariski dense for $X^{(d)} \neq \emptyset$.

(iii) Let $U_\gamma := \text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ and note that $U := \bigcap_{\gamma \in \Sigma_d(1, \dots, n)} U_\gamma$ is contained in $X^{(\geq d+1)}$. Indeed, the presence of $a \in U \setminus X^{(\geq d+1)} = U \cap X^{(\leq d)}$ implies the existence of a tangent vector $v(a) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ of weight $\leq d$. The support of $v(a)$ is contained in some $\gamma \in \Sigma_d(1, \dots, n)$ and $0^n \neq v(a) \in \ker \Pi_\gamma = \ker(d\Pi_\gamma)_a$. That contradicts $a \in \text{Etale}(\Pi_\gamma)$ and justifies that $U \subseteq X^{(\geq d+1)}$.

We claim that U is Zariski dense in X . To this end, observe that $U \subseteq U_\gamma$ implies $I(U_\gamma, \overline{\mathbb{F}_q}) \subseteq I(U, \overline{\mathbb{F}_q})$ for $\forall \gamma \in \Sigma_d(1, \dots, n)$. Therefore

$$I(U, \overline{\mathbb{F}_q}) \supseteq \sum_{\gamma \in \Sigma_d(1, \dots, n)} I(U_\gamma, \overline{\mathbb{F}_q})$$

and the Zariski closure

$$\begin{aligned} \overline{U} &= VI(U, \overline{\mathbb{F}_q}) \subseteq V \left(\sum_{\gamma \in \Sigma_d(1, \dots, n)} I(U_\gamma, \overline{\mathbb{F}_q}) \right) = \\ &= \bigcap_{\gamma \in \Sigma_d(1, \dots, n)} VI(U_\gamma, \overline{\mathbb{F}_q}) = \bigcap_{\gamma \in \Sigma_d(1, \dots, n)} \overline{U_\gamma} = \bigcap_{\gamma \in \Sigma_d(1, \dots, n)} X = X. \end{aligned}$$

Now $X = \overline{U} \subseteq \overline{X^{(\geq d+1)}} \subseteq X$ reveals the Zariski density of $X^{(\geq d+1)}$ in X . □

The proof of Proposition 2 (iii) reveals that for any point $a \in X^{(d)}$ there exists a d -tuple of indices $\gamma \in \Sigma_d(1, \dots, n)$, such that the puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ is not etale at a .

In the light of Proposition 2, the finite Zariski tangent spaces are expected to suit for construction of extremal codes.

Corollary 3. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible k -dimensional affine variety, defined over \mathbb{F}_q . Suppose that there exist $i \in \{1, \dots, n\}$ and $\beta \subseteq \{1, \dots, n\} \setminus \{i\}$ with $|\beta| = d$, such that $\Pi_\beta : X \rightarrow \Pi_\beta(X)$ is a non-finite morphism and for any $\delta \in \Sigma_d(1, \dots, n)$ with $i \in \delta$ the puncturing $\Pi_\delta : X \rightarrow \Pi_\delta(X)$ is a finite separable morphism. Then $\Pi_i : X \rightarrow \Pi_i(X)$ is a finite separable morphism, the generic tangent codes to X are $[n, k, d]$ -codes and the generic finite Zariski tangent spaces to $\Pi_i(X)$ are $[n-1, k, d]$ -codes.*

Proof. For any $\gamma \subseteq \{1, \dots, n\} \setminus \{i\}$ with $|\gamma| = d-1$ note that $\Pi_{\gamma \cup \{i\}} : X \rightarrow \Pi_{\gamma \cup \{i\}}(X)$

is a finite and separable puncturing. The factorization

$$\begin{array}{ccc} X & \xrightarrow{\Pi_i} & \Pi_i(X) \\ \Pi_{\gamma \cup \{i\}} \downarrow & \searrow \Pi_\gamma & \\ \Pi_{\gamma \cup \{i\}}(X) & & \end{array}$$

implies the inclusions $\overline{\mathbb{F}_q}(\Pi_{\gamma \cup \{i\}}(X)) \subseteq \overline{\mathbb{F}_q}(\Pi_i(X)) \subseteq \overline{\mathbb{F}_q}(X)$ of the corresponding function fields. The extensions $\overline{\mathbb{F}_q}(\Pi_{\gamma \cup \{i\}}(X)) \subseteq \overline{\mathbb{F}_q}(\Pi_i(X))$ and $\overline{\mathbb{F}_q}(\Pi_i(X)) \subseteq \overline{\mathbb{F}_q}(X)$ are finite and separable, as far as $\overline{\mathbb{F}_q}(\Pi_{\gamma \cup \{i\}}(X)) \subseteq \overline{\mathbb{F}_q}(X)$ is finite and separable. Thus, $\Pi_i : X \rightarrow \Pi_i(X)$ is a finite separable morphism and the generic tangent codes to $\Pi_i(X)$ are of minimum distance $\geq d$ by Proposition 2 (iii).

We claim that $\Pi_\beta : \Pi_i(X) \rightarrow \Pi_{\beta \cup \{i\}}(X)$ is a non-finite puncturing at $|\beta| = d$ variables. To this end, consider the commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\Pi_i} & \Pi_i(X) \\ \Pi_\beta \downarrow & \searrow \Pi_{\beta \cup \{i\}} & \downarrow \Pi_\beta \\ \Pi_\beta(X) & \xrightarrow{\Pi_i} & \Pi_{\beta \cup \{i\}}(X) \end{array} .$$

By assumption, $\Pi_\beta : X \rightarrow \Pi_\beta(X)$ is a non-finite puncturing at d variables, so that $\Pi_{\beta \cup \{i\}} : \Pi_i \Pi_\beta : X \rightarrow \Pi_{\beta \cup \{i\}}(X)$ is a non-finite puncturing at $d + 1$ variables. The presence of a factorization $\Pi_{\beta \cup \{i\}} = \Pi_\beta \Pi_i : X \rightarrow \Pi_{\beta \cup \{i\}}(X)$ through a finite morphism $\Pi_i : X \rightarrow \Pi_i(X)$ suffices for $\Pi_\beta : \Pi_i(X) \rightarrow \Pi_{\beta \cup \{i\}}(X)$ to be a non-finite morphism. Now, Proposition 2 (ii) applies to provide an upper bound d on the minimum distance of all the finite Zariski tangent spaces to $\Pi_i(X)$. As a result, the generic tangent codes to $\Pi_i(X)$ are of length $n - 1$, dimension k and minimum distance d .

□

If $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ is an irreducible affine variety, defined over \mathbb{F}_q with a non-finite puncturing $\Pi_\beta : X \rightarrow \Pi_\beta(X)$ at $|\beta| = d$ coordinates and finite separable puncturings $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ for $\forall \gamma \in \Sigma_{d-1}(1, \dots, n)$ then the finite Zariski tangent spaces to X are of minimum distance d at "almost all" the points of X (i.e., on a Zariski dense subset of X). For fixed length n and minimum distance d one looks for tangent codes of maximal dimension. These occur at the singular points $a \in X$, at which the parity check matrix of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ is of minimum rank.

If the length n and the dimension k are fixed then one looks for a k -dimensional irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, which is in "most general" position with respect to the coordinate axes. Namely, we seek such equations of X which maximize the minimal integer $d \in \mathbb{N}$, for which there is a non-finite puncturing $\Pi_\beta : X \rightarrow \Pi_\beta(X)$ of X at $|\beta| = d$ variables.

3.2 Reproducing the dimension and the minimum distance of a code

The Zariski tangent bundles of the coordinate k -dimensional affine subspace $X_0 := V(x_{k+1}, \dots, x_n) \subset \overline{\mathbb{F}_q}^n$ are constant, i.e., $T_a(X, F) = F^k \times 0^{n-k}$ for any point $a \in X$ and any field $\mathbb{F}_q^{\delta(a)} \subseteq F \leq \overline{\mathbb{F}_q}$. The next corollary provides different embeddings X of $\overline{\mathbb{F}_q}^k$ in $\overline{\mathbb{F}_q}^n$ with non-constant Zariski tangent bundles $T(X, F)$. For any natural number $d \leq n - k$ and any $\sigma \in \Sigma_d(1, \dots, n)$ we construct such $X \simeq \overline{\mathbb{F}_q}^k$ that $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ contains a non-zero word $v(a)$ of $\text{Supp}(v(a)) \subseteq \sigma$ for any $a \in X$. For an arbitrary \mathbb{F}_q -linear $[n, k, d]$ -code C we provide explicit equations of $\overline{\mathbb{F}_q}^k \simeq X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, such that "almost all" tangent codes to X are $[n, k, d]$ -codes

Corollary 4. *Let C be an $[n, k, d]$ -code and $\sigma \in \Sigma_d(1, \dots, n)$ be a support of a non-zero word $c \in C \setminus \{0^n\}$. Then there is an irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ through 0^n with $T_{0^n}(X, \mathbb{F}_q) = C$, isomorphic to $\overline{\mathbb{F}_q}^k$ and such that $T_a(X, \mathbb{F}_{q^{\delta(a)}}) \simeq \mathbb{F}_{q^{\delta(a)}}^k$ contains a word $v(a) \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \setminus \{0^n\}$ of $\text{Supp}(v(a)) \subseteq \sigma$ for all $a \in X$.*

In particular, $X = X^{(\leq d)}$ and $\emptyset \neq X^{(d)} \cap X^{\text{smooth}} = X^{(\geq d)} \cap X^{\text{smooth}}$ is such a non-empty, Zariski open, Zariski dense subset of X that the Zariski tangent spaces $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ are $[n, k, d]$ -codes for all $a \in X^{(d)} \cap X^{\text{smooth}}$.

Proof. Let $H \in M_{(n-k) \times n}(\mathbb{F}_q)$ be a parity check matrix of C with columns $H_i \in M_{(n-k) \times 1}(\mathbb{F}_q)$. Since $\text{rk} H = n - k$, there exists $\alpha \in \Sigma_{n-k}(1, \dots, n)$ with $\det(H_\alpha) = \det(H_{\alpha_1} \dots H_{\alpha_{n-k}}) \neq 0$. Without loss of generality, one can assume that $H_\alpha = (H_{\alpha_1} \dots H_{\alpha_{n-k}}) = I_{n-k}$ for the identity matrix I_{n-k} of size $n - k$ or

$$H_{i, \alpha_j} = \delta_{ij} = \begin{cases} 1 & \text{for } 1 \leq i = j \leq n - k, \\ 0 & \text{for } 1 \leq i \neq j \leq n - k. \end{cases}$$

The presence of a word $c \in C$ with $\text{Supp}(c) = \sigma \in \Sigma_d(1, \dots, n)$ implies that $H_{\sigma_\nu} \in \text{Span}_{\mathbb{F}_q}(H_{\sigma_1}, \dots, H_{\sigma_{\nu-1}}, H_{\sigma_{\nu+1}}, \dots, H_{\sigma_d})$ for all $1 \leq \nu \leq d$. We claim that the existence of $\sigma_\nu \notin \alpha$, since $\sigma \subseteq \alpha$ contradicts the linear dependence of the columns $H_{\sigma_1}, \dots, H_{\sigma_d}$. If $H_{\sigma_\nu} = \sum_{s \in \sigma \setminus \{\sigma_\nu\}} \lambda_s H_s$ for $\sigma_\nu \notin \alpha$ and some $\lambda_s \in \mathbb{F}_q$, then we choose polynomials

$$f_{i, \alpha_j}(x_{\alpha_j}) = H_{i, \alpha_j} x_{\alpha_j} = \delta_{ij} x_{\alpha_j} \in \mathbb{F}_q[x_{\alpha_j}] \quad \text{for } \forall 1 \leq i, j \leq n - k,$$

$$f_{i, s}(x_s) = H_{i, s} x_s + \sum_{r \geq 2} a_{i, s, r} x_s^r \in \mathbb{F}_q[x_s] \quad \text{for } \forall 1 \leq i \leq n - k, \quad \forall s \in \{1, \dots, n\} \setminus (\alpha \cup \{\sigma_\nu\})$$

and

$$f_{i, \sigma_\nu}(x_{\sigma_\nu}) = \sum_{s \in \sigma \setminus \{\sigma_\nu\}} \lambda_s f_{i, s}(x_{\sigma_\nu}) \in \mathbb{F}_q[x_{\sigma_\nu}] \quad \text{for } \forall 1 \leq i \leq n - k.$$

The polynomials

$$f_i(x_1, \dots, x_n) := \sum_{s=1}^n f_{i, s}(x_s) = x_{\alpha_i} + \sum_{s \in \{1, \dots, n\} \setminus \alpha} f_{i, s}(x_s) \quad \text{for } 1 \leq i \leq n - k$$

cut out an affine variety $X = V(f_1, \dots, f_{n-k}) \subset \overline{\mathbb{F}_q}^n$ with a biregular puncturing $\Pi_\alpha : X \rightarrow \overline{\mathbb{F}_q}^k$ at $\alpha \in \Sigma_{n-k}(1, \dots, n)$. In particular, X is irreducible and the polynomials $f_1, \dots, f_{n-k} \in \mathbb{F}_q[x_1, \dots, x_n]$ generate the absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_{n-k} \rangle_{\overline{\mathbb{F}_q}}$ of X . According to

$$\begin{aligned} \frac{\partial f_i}{\partial x_{\sigma_\nu}} &= \frac{\partial f_{i, \sigma_\nu}}{\partial x_{\sigma_\nu}}(x_{\sigma_\nu}) = \sum_{s \in \sigma \setminus \{\sigma_\nu\}} \lambda_s \frac{\partial f_{i, s}}{\partial x_{\sigma_\nu}}(x_{\sigma_\nu}) = \sum_{s \in \sigma \setminus \{\sigma_\nu\}} \lambda_s \frac{\partial f_{i, s}}{\partial x_s} \Big|_{x_s = x_{\sigma_\nu}} \\ &= \sum_{s \in \sigma \setminus \{\sigma_\nu\}} \lambda_s \frac{\partial f_i}{\partial x_s} \quad \text{for } \forall 1 \leq i \leq n-k, \end{aligned}$$

one has

$$\frac{\partial f}{\partial x_{\sigma_\nu}}(a) = \sum_{s \in \sigma \setminus \{\sigma_\nu\}} \lambda_s \frac{\partial f}{\partial x_s}(a) \quad \text{for } \forall a \in X,$$

whereas $\text{rk} \frac{\partial f}{\partial x_\sigma}(a) < d$. In other words, $v(a) \in \mathbb{F}_{q^{\delta(a)}}^n$ with $v(a)_s := \lambda_s$ for $s \in \sigma \setminus \{\sigma_\nu\}$, $v(a)_{\sigma_\nu} := -1$ and $v(a)_s := 0$ for $s \in \{1, \dots, n\} \setminus \sigma$ belongs to $T_a(X, \mathbb{F}_{q^{\delta(a)}}) \setminus \{0^n\}$ and has $\text{Supp}(v(a)) \subseteq \sigma$ for $\forall a \in X$. Straightforwardly,

$$\frac{\partial f_i}{\partial x_s}(0^n) = \frac{\partial f_{i, s}}{\partial x_s}(0) = H_{i, s} \quad \text{for } \forall 1 \leq i \leq n-k, \forall 1 \leq s \leq n$$

reveals that $\frac{\partial f}{\partial x}(0^n) = H$ and $T_{0^n}(X, \mathbb{F}_q) = C$.

The equality $X = X^{(\leq d)}$ is an immediate consequence of Proposition 2 (iii). By Proposition 2 (ii) and $T_{0^n}(X, \mathbb{F}_q) = C$, $X^{(d)} = X^{(\geq d)}$ is a non-empty, Zariski open, Zariski dense subset of X . Due to the irreducibility of X , it intersects the smooth locus in a non-empty, Zariski open, Zariski dense subset $X^{(d)} \cap X^{\text{smooth}}$ of X . \square

3.3 Tangent bundle interpolation of a finite family of codes

The next proposition illustrates how linear codes of arbitrary minimum distance can be interpolated by a finite Zariski tangent bundle.

Proposition 5. *Let $\mathcal{C} \rightarrow S$ be a family of \mathbb{F}_q -linear codes $\mathcal{C}(a) \subset \mathbb{F}_q^n$, $a \in S$ of length n , dimension $k = \dim_{\mathbb{F}_q} \mathcal{C}(a)$ and arbitrary minimum distance $d(\mathcal{C}(a)) \leq n + 1 - k$, parameterized by a subset $S \subseteq \mathbb{F}_q^n$. Then there exist irreducible k -dimensional affine varieties $Y_1/\mathbb{F}_q, \dots, Y_s/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ with*

$$\mathbb{F}_q^n \subset Y_1 \cup \dots \cup Y_s, \quad S \subseteq Y_1^{\text{smooth}}(\mathbb{F}_q) \cup \dots \cup Y_s^{\text{smooth}}(\mathbb{F}_q),$$

such that $T_a(Y_i, \mathbb{F}_q) = \mathcal{C}(a)$ for all $a \in S$ and all $Y_i \ni a$.

Proof. Let us choose a family $\mathcal{H} \rightarrow S$ of parity-check matrices $\mathcal{H}(a) \in M_{(n-k) \times n}(\mathbb{F}_q)$ of $\mathcal{C}(a) \subset \mathbb{F}_q^n$ for all $a \in S$ and denote by $\mathcal{H}(a)_{ij} \in \mathbb{F}_q$ the entries of these matrices. For an arbitrary $\beta \in \mathbb{F}_q$, consider the Lagrange basis polynomial

$$L_{\mathbb{F}_q}^\beta(t) := \prod_{\alpha \in \mathbb{F}_q \setminus \{\beta\}} \frac{t - \alpha}{\beta - \alpha}$$

with $L_{\mathbb{F}_q}^\beta(t)(\beta) = 1$ and $L_{\mathbb{F}_q}^\beta(t)|_{\mathbb{F}_q \setminus \{\beta\}} = 0$. Straightforwardly,

$$L_{\mathbb{F}_q}^0(t) := \left[\prod_{\alpha \in \mathbb{F}_q^*} (t - \alpha) \right] \left\{ \left[\prod_{\alpha \in \mathbb{F}_q^*} (t - \alpha) \right] \Big|_{t=0} \right\}^{-1} = \\ (t^{q-1} - 1)(-1)^{-1} = -(t^{q-1} - 1).$$

Towards an explicit calculation of $L_{\mathbb{F}_q}^\beta(t)$ for $\beta \in \mathbb{F}_q^*$, let us denote by $\sigma_1, \dots, \sigma_{q-1}$ the elementary symmetric polynomials of the roots of $f(t) := \prod_{\alpha \in \mathbb{F}_q^*} (t - \alpha) = t^{q-1} - 1$.

Put $\tau_1, \dots, \tau_{q-2}$ for the elementary symmetric polynomials of the roots of the monic polynomial

$$f_\beta(t) := \prod_{\alpha \in \mathbb{F}_q^* \setminus \{\beta\}} (t - \alpha) = \frac{f(t)}{t - \beta} = \frac{t^{q-1} - 1}{t - \beta} = t^{q-2} + \sum_{s=0}^{q-3} (-1)^{q-2-s} \tau_{q-2-s} t^s.$$

Then the relations

$$\begin{aligned} \tau_1 + \beta &= \sigma_1 = 0, \\ \tau_s + \beta \tau_{s-1} &= \sigma_s = 0 \quad \text{for } \forall 2 \leq s \leq q-2 \quad \text{and} \\ \beta \tau_{q-2} &= \sigma_{q-1} = (-1)^q, \end{aligned}$$

reveal that $\tau_s = (-\beta) \tau_{s-1}$ for $\forall 1 \leq s \leq q-2$, $\tau_0 := 1$ form a geometric progression $\{\tau_s\}_{s=1}^{q-2}$ with quotient $(-\beta)$. As a result,

$$\tau_s = (-\beta)^s \quad \text{for } \forall 1 \leq s \leq q-2$$

and

$$f_\beta(t) = t^{q-2} + \sum_{s=0}^{q-3} \beta^{q-2-s} t^s = t^{q-2} + \sum_{s=0}^{q-3} \beta^{-s-1} t^s,$$

according to $\beta^{q-2} = \beta^{-1}$ for $\forall \beta \in \mathbb{F}_q^*$. Now,

$$\begin{aligned} L_{\mathbb{F}_q}^\beta(t) &:= \frac{t f_\beta(t)}{\beta f_\beta(\beta)} = \frac{t^{q-1} + \sum_{s=1}^{q-2} \beta^{-s} t^s}{\beta^{q-1} + \sum_{s=1}^{q-2} 1} \\ &= (q-1)^{-1} \left[t^{q-1} + \sum_{s=1}^{q-2} \beta^{-s} t^s \right] = - \left[t^{q-1} + \sum_{s=1}^{q-2} \beta^{-s} t^s \right] \end{aligned}$$

for arbitrary $\beta \in \mathbb{F}_q^*$.

Let us denote by

$$\begin{aligned} \Phi_p : \overline{\mathbb{F}_q}^n &\longrightarrow \overline{\mathbb{F}_q}^n, \\ \Phi_p(a_1, \dots, a_n) &= (a_1^p, \dots, a_n^p) \quad \text{for } \forall a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n \end{aligned}$$

the Frobenius automorphism of degree $p = \text{char} \mathbb{F}_q$ and consider the polynomials

$$f_i(x_1, \dots, x_n) := \sum_{b \in \Phi_p(S)} \left[\sum_{j=1}^n \mathcal{H}(\Phi_p^{-1}(b))_{ij} (x_j - x_j^q) \right] L_{\mathbb{F}_q}^{b_1}(x_1^p) \dots L_{\mathbb{F}_q}^{b_n}(x_n^p) \in \mathbb{F}_q[x_1, \dots, x_n]$$

for $1 \leq i \leq n - k$. Suppose that the $X := V(f_1, \dots, f_{n-k}) \subset \overline{\mathbb{F}_q}^n$ decomposes into a union $X = Y_1 \cup \dots \cup Y_s$ of its irreducible components Y_i . We claim that Y_1, \dots, Y_s satisfy the announced conditions. First of all, $\mathbb{F}_q^n \subset X$, as far as an arbitrary point $a = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ has components $a_j = a_j^q$ and $f_i(a_1, \dots, a_n) = 0$ for $\forall 1 \leq i \leq n - k$. The partial derivatives are

$$\frac{\partial f_i}{\partial x_j} = \sum_{b \in \Phi_p(S)} \mathcal{H}(\Phi_p^{-1}(b))_{ij} L_{\mathbb{F}_q}^{b_1}(x_1^p) \dots L_{\mathbb{F}_q}^{b_n}(x_n^p)$$

and their values at $a \in S$ equal

$$\frac{\partial f_i}{\partial x_j}(a) = \mathcal{H}(\Phi_p^{-1} \Phi_p(a))_{ij} = \mathcal{H}(a)_{ij}.$$

Note that the composition of Lagrange interpolation polynomials with the Frobenius automorphism Φ_p is designed in such a way that to adjust

$$\frac{\partial(f_1, \dots, f_{n-k})}{\partial(x_1, \dots, x_n)}(a) = \mathcal{H}(a)$$

at all the points $a \in S$. For an arbitrary point $a \in S \subset X(\mathbb{F}_q) := X \cap \mathbb{F}_q^n$ let Y_i be an irreducible component of X through a . The Zariski tangent space $T_a(Y_i, \mathbb{F}_q)$ is contained in the right null-space $\mathcal{C}(a)$ of the Jacobian matrix $\frac{\partial(f_1, \dots, f_{n-k})}{\partial(x_1, \dots, x_n)}(a) = \mathcal{H}(a)$. On the other hand, $\dim Y_i \geq n - (n - k) = k$, as far as Y_i is subject to at least $n - k$ polynomial equations $f_1 = \dots = f_{n-k} = 0$. Thus,

$$k \leq \dim Y_i \leq \dim_{\mathbb{F}_q} T_a(Y_i, \mathbb{F}_q) \leq \dim_{\mathbb{F}_q} \mathcal{C}(a) = k$$

implies that $\mathcal{C}(a) = T_a(Y_i, \mathbb{F}_q)$, $\dim Y_i = k$ and any $a \in Y_i^{\text{smooth}}(\mathbb{F}_q)$. □

Algorithms for primary decomposition of polynomial ideals and decomposition of an affine variety into a union of irreducible components are provided by [1], [6], [5], [18], [15], [10], [13] and other sources.

4 Decoding and deforming tangent codes. Gradient codes. ■

4.1 Simultaneous decoding tangent codes

After organizing linear codes in families, constituting tangent bundles to affine varieties, we propose an algorithm for simultaneous decoding of tangent codes, after recognizing the support of the error of the received word.

Let $C \subset \mathbb{F}_q^n$ be an \mathbb{F}_q -linear code of minimum distance d . A word $w \in \mathbb{F}_q^n$ has a C -error of weight $\leq t$ if there exists $e \in \mathbb{F}_q^n$ of weight $\text{wt}(e) \leq t$ with $w - e \in C$. Denote by

$$\text{Err}(C, t) := \{w \in \mathbb{F}_q^n \mid \exists e \in \mathbb{F}_q^n, \text{wt}(e) \leq t, w - e \in C\}$$

the set of the words with a C -error of weight $\leq t$. Note that $\text{Err}(C, t) \supset C$ and $\text{Err}(C, t)/C := \{w + C \mid w \in \text{Err}(C, t)\}$ consists of the cosets, whose leaders are of weight $\leq t$. We say that $w \in \mathbb{F}_q^n$ has a C -error, supported by $i \in \Sigma_t(1, \dots, n)$ if there is $e \in \mathbb{F}_q^n$ with $\text{Supp}(e) \subseteq i$ and $w - e \in C$. It is well known that if t does not exceed the integral part $\lfloor \frac{d-1}{2} \rfloor$ of $\frac{d-1}{2}$ and $w \in \mathbb{F}_q^n$ has a C -error of weight $\leq t$ then $e \in \mathbb{F}_q^n$ with $\text{wt}(e) \leq t$ and $w - e \in C$ is unique.

Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over \mathbb{F}_q with $X^{(\geq 2t+1)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \geq 2t+1\} \neq \emptyset$ for some $t \in \mathbb{N}$. The disjoint union

$$\text{Err}(TX, t) := \coprod_{a \in X^{(2t+1)}} \text{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), t)$$

of the words $\text{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), t)$ with $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error of weight $\leq t$ will be called the bundle of the words with TX -error of weight $\leq t$. Denote by

$$\pi : \text{Err}(TX, t) \longrightarrow X^{(2t+1)}$$

the natural projection on the base. To any $i \in \Sigma_t(1, \dots, n)$ we associate a polynomial matrix $A_i(x) \in M_{l_i \times t}(\mathbb{F}_q[x_1, \dots, x_n])$ for some $l_i \in \mathbb{N}$, such that $w_a \in \pi^{-1}(a) = \text{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), t)$ has a $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error $e_a \in \mathbb{F}_{q^{\delta(a)}}^n$, supported by i exactly when $A_i(a)w_a^t = 0$. If so, then e_a can be computed explicitly by the means of the Jacobian matrix $\frac{\partial f}{\partial x}(a)$ of a generating set $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ of $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ at a . The aforementioned result is referred to as a simultaneous decoding of tangent codes, as far as the construction of $A_i(x)$ for $\forall i \in \Sigma_t(1, \dots, n)$ allows to recognize simultaneously the supports of the $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -errors for all $a \in X$ and to obtain the corresponding errors from $\text{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), t)$.

Towards the construction of $A_i(x)$ we need the following

Lemma 6. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety with absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$, generated by $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$, $i \in \Sigma_t(1, \dots, n)$ and $G_{i, \neg i}$ be a Groebner basis of $I(X, \mathbb{F}_q) = \langle f_1, \dots, f_m \rangle_{\mathbb{F}_q}$ with respect to a lexicographic order of $\mathbb{F}_q[x_1, \dots, x_n]$ with $x_i >_{\text{lex}} x_{\neg i}$, obtained by Buchberger's algorithm. Then:*

$$(i) \quad G_{i, \neg i} \subseteq M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n]) \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix};$$

(ii) *the absolute ideal $I(\Pi_i(X), \overline{\mathbb{F}_q}) = I(\overline{\Pi_i(X)}, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_{\neg i}]$ of the Zariski closure $\overline{\Pi_i(X)}$ of $\Pi_i(X)$ is generated by $G_{\neg i} := G_{i, \neg i} \cap \mathbb{F}_q[x_{\neg i}]$.*

Proof. (i) Let $f := (f_1, \dots, f_m) \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$. By an induction on the steps of Buchberger's algorithm, we show that any entry of the current generating set Δ of $I(X, \mathbb{F}_q)$ is of the form gf^t for some $g = (g^{(1)}, \dots, g^{(m)}) \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$.

Let $e_j \in M_{1 \times m}(\mathbb{F}_q)$ be the ordered m -tuple with unique non-zero entry 1 at the j -th position. One can view e_j as an ordered m -tuple of polynomials. At the input, any f_j is expressed as a product $e_j f^t$ with the transposed f^t of $f = (f_1, \dots, f_m) \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$.

For arbitrary $h_1, h_2 \in \mathbb{F}_q[x_1, \dots, x_n]$ let x^γ be the least common multiple of the leading monomials $LM(h_1), LM(h_2)$ with respect to the fixed lexicographic order on $\mathbb{F}_q[x_1, \dots, x_n]$. If $LT(h_j) = LC(h_j)LM(h_j)$ are the leading terms of h_j then the S -polynomial of h_1, h_2 (or the syzygy polynomial of h_1, h_2) is defined as

$$S(h_1, h_2) = \frac{x^\gamma}{LT(h_1)} h_1 - \frac{x^\gamma}{LT(h_2)} h_2.$$

If there exist $g_j \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$ with $h_j = g_j f^t$ then

$$S(h_1, h_2) = \left(\frac{x^\gamma}{LT(h_1)} g_1 - \frac{x^\gamma}{LT(h_2)} g_2 \right) f^t$$

can also be represented as a product of a row m -tuple of polynomials with the column $f^t = (f_1, \dots, f_m)^t$. At each step, Buchberger's algorithm for obtaining a Groebner basis of $I(X, \mathbb{F}_q)$ adjoins to the current generating set Δ of $I(X, \mathbb{F}_q)$ the remainders $\overline{S(h_1, h_2)}^\Delta$ of the S -polynomials of $h_1, h_2 \in \Delta$ under the division by Δ . By its very definition,

$$\overline{S(h_1, h_2)}^\Delta = S(h_1, h_2) - a f^t$$

for some $a \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$ and no-one monomial of $\overline{S(h_1, h_2)}^\Delta$ with non-zero coefficient is divisible by $LT(h)$ for $h \in \Delta$. Thus, if all $h \in \Delta$ are represented in the form $h = gf^t$ for some $g \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$, then all $\overline{S(h_1, h_2)}^\Delta$ with $h_1, h_2 \in \Delta$ are of the same form and adjoining them to Δ , one gets a set of polynomials $\Delta' \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n]) f^t$.

Buchberger's algorithm terminates with the Groebner basis $G_{i, \neg i} = \Delta$, once $\overline{S(h_1, h_2)}^\Delta = 0$ for $\forall h_1, h_2 \in \Delta$.

(ii) Combining the Closure Theorem 3 from Chapter 3, § 2 [3] with the Elimination Theorem 2 from Chapter 3, § 1 [3], one concludes that the Zariski closure of $\Pi_i(X)$ is the affine variety $\overline{\Pi_i(X)} = V(G_{\neg i})$. Therefore, the absolute ideal

$$I(\Pi_i(X), \overline{\mathbb{F}_q}) = IVI(\Pi_i(X), \overline{\mathbb{F}_q}) = I(\overline{\Pi_i(X)}, \overline{\mathbb{F}_q}) = IV(G_{\neg i}, \overline{\mathbb{F}_q}) = r\langle G_{\neg i} \rangle_{\overline{\mathbb{F}_q}}$$

equals the radical $r\langle G_{\neg i} \rangle_{\overline{\mathbb{F}_q}} \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$ of $\langle G_{\neg i} \rangle_{\overline{\mathbb{F}_q}}$. If $h(x_{\neg i}) \in r\langle G_{\neg i} \rangle_{\overline{\mathbb{F}_q}}$ then

$$h(x_{\neg i})^N \in \langle G_{\neg i} \rangle_{\overline{\mathbb{F}_q}} \subset \langle G_{\neg i} \rangle_{\overline{\mathbb{F}_q}} \otimes_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}[x_1, \dots, x_n] \subseteq \langle G_{i, \neg i} \rangle_{\overline{\mathbb{F}_q}} = I(X, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n]$$

for some $N \in \mathbb{N}$. The absolute ideal $I(X, \overline{\mathbb{F}_q})$ of the irreducible affine variety X is prime and therefore radical, i.e., $I(X, \overline{\mathbb{F}_q}) = rI(X, \overline{\mathbb{F}_q})$. As a result, $h(x_{\neg i}) \in$

$I(X, \overline{\mathbb{F}}_q)$ and bearing in mind that $h(x_{-i}) \in \overline{\mathbb{F}}_q[x_{-i}]$, one concludes that $h(x_{-i}) \in I(X, \overline{\mathbb{F}}_q) \cap \overline{\mathbb{F}}_q[x_{-i}]$. Buchberger's algorithm for obtaining the Groebner basis $G_{i,-i}$ of $I(X, \overline{\mathbb{F}}_q) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}}_q}$ adjoins to $\{f_1, \dots, f_m\}$ the remainders of appropriate S -polynomials and does not depend on the constant field \mathbb{F}_q . Bearing in mind that f_1, \dots, f_m generate the absolute ideal $I(X, \overline{\mathbb{F}}_q) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}}_q}$ of X , one concludes that $G_{i,-i}$ is a Groebner basis of $I(X, \overline{\mathbb{F}}_q)$. By the Elimination Theorem 2 from Chapter 3, §1 [3], $G_{i,-i} \cap \overline{\mathbb{F}}_q[x_{-i}] = G_{i,-i} \cap \mathbb{F}_q[x_{-i}] = G_{-i}$ is a Groebner basis of $I(X, \overline{\mathbb{F}}_q) \cap \overline{\mathbb{F}}_q[x_{-i}]$ with respect to the fixed lexicographic order of $\overline{\mathbb{F}}_q[x_{-i}]$. Thus,

$$h(x_{-i}) \in I(X, \overline{\mathbb{F}}_q) \cap \overline{\mathbb{F}}_q[x_{-i}] = \langle G_{-i} \rangle_{\overline{\mathbb{F}}_q}$$

and $r\langle G_{-i} \rangle_{\overline{\mathbb{F}}_q} \subseteq \langle G_{-i} \rangle_{\overline{\mathbb{F}}_q}$. Combining with $\langle G_{-i} \rangle_{\overline{\mathbb{F}}_q} \subseteq r\langle G_{-i} \rangle_{\overline{\mathbb{F}}_q}$ one concludes that $I(\Pi_i(X), \overline{\mathbb{F}}_q) = I(\overline{\Pi_i(X)}, \overline{\mathbb{F}}_q) = r\langle G_{-i} \rangle_{\overline{\mathbb{F}}_q} = \langle G_{-i} \rangle_{\overline{\mathbb{F}}_q}$. \square

In order to characterize the words $w \in \mathbb{F}_{q^{\delta(a)}}^n$, whose $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error is supported by $i \in \Sigma_t(1, \dots, n)$, let us note that the puncturing Π_i can be viewed, both, as a morphism $\Pi_i : \overline{\mathbb{F}}_q^n \rightarrow \overline{\mathbb{F}}_q^{n-t}$ of $\overline{\mathbb{F}}_q^n$ and a morphism $\Pi_i : X \rightarrow \Pi_i(X)$ of the irreducible affine variety X . If $\overline{\Pi_i(X)} \subset \overline{\mathbb{F}}_q^{n-t}$ is the Zariski closure of $\Pi_i(X)$ in $\overline{\mathbb{F}}_q^{n-t}$ then

$$\Pi_i^{-1}(\overline{\Pi_i(X)}) := \{a \in \overline{\mathbb{F}}_q^n \mid \Pi_i(a) \in \overline{\Pi_i(X)}\}$$

is an irreducible affine variety of $\overline{\mathbb{F}}_q^n$, isomorphic to $\overline{\Pi_i(X)} \times \overline{\mathbb{F}}_q^t$ and containing X . We call $\Pi_i^{-1}(\overline{\Pi_i(X)})$ the cylinder over $\overline{\Pi_i(X)}$.

Proposition 7. *Let $X \subset \overline{\mathbb{F}}_q^n$ be an affine variety, whose absolute ideal $I(X, \overline{\mathbb{F}}_q) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}}_q}$ is generated by some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$, $i \in \Sigma_t(1, \dots, n)$ and $\Pi_i^{-1}(\overline{\Pi_i(X)}) \simeq \overline{\Pi_i(X)} \times \overline{\mathbb{F}}_q^t$ be the cylinder over $\overline{\Pi_i(X)}$. Suppose that the tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ to X at $a \in X$ is of minimum distance $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) > t$ and $w \in \mathbb{F}_{q^{\delta(a)}}^n$ is a word with a $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error of weight $\leq t$. Then the $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error of w is supported by i if and only if $w \in T_a(\Pi_i^{-1}(\overline{\Pi_i(X)}), \mathbb{F}_{q^{\delta(a)}})$ is tangent to the cylinder $\Pi_i^{-1}(\overline{\Pi_i(X)})$ at a . If so, then any $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error $e \in \mathbb{F}_{q^{\delta(a)}}^n$ of w with $\Pi_i(e) = 0_{(n-t) \times 1}$ projects onto a solution $\Pi_{-i}(e) = (e_{i_1}, \dots, e_{i_t}) = e_i$ of the homogeneous linear system*

$$\frac{\partial f}{\partial x_i}(a) \begin{pmatrix} x_{i_1} \\ \dots \\ x_{i_t} \end{pmatrix} = \frac{\partial f}{\partial x}(a) w^t.$$

Proof. The Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ does not contain a non-zero word $v(a)$ of $\text{Supp}(v(a)) \subseteq i \in \Sigma_t(1, \dots, n)$, according to $t < d(T_a(X, \mathbb{F}_{q^{\delta(a)}}))$. By Lemma 1 (i), one concludes that $\Pi_i : X \rightarrow \Pi_i(X)$ is etale at $a \in \Pi_i^{-1}(\Pi_i(X))^{\text{smooth}} \cap \mathbb{F}_{q^{\delta(a)}}^n$. Now Lemma 1 (ii) applies to provide the surjectiveness of the differential

$$(d\Pi_i)_a : T_a(X, F) \longrightarrow T_{\Pi_i(a)}(\Pi_i(X), F). \quad (2)$$

Let $G_{i,-i}$ be a Groebner basis of $I(X, \mathbb{F}_q) = \langle f_1, \dots, f_m \rangle_{\mathbb{F}_q}$ with respect to a lexicographic order with $x_i >_{\text{lex}} x_{-i}$, obtained by Buchberger's algorithm. If $G_{-i} := G_{i,-i} \cap \mathbb{F}_q[x_{-i}] = \{h_1, \dots, h_l\}$ and $f = (f_1, \dots, f_m) \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$ then by Lemma 6 (i) there exist $g_1, \dots, g_l \in M_{1 \times m}(\mathbb{F}_q[x_1, \dots, x_n])$ with $h_i = g_i f^t$ for $\forall 1 \leq i \leq l$. Consider the matrix $\mathcal{G}_i \in M_{l \times m}(\mathbb{F}_q[x_1, \dots, x_n])$ with rows g_1, \dots, g_l . We claim that the existence of $e \in \mathbb{F}_{q^{\delta(a)}}^n$ with $\text{Supp}(e) \subseteq i$ and $w - e \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ is equivalent to

$$\mathcal{G}_i(a) \frac{\partial f^t}{\partial x}(a) w^t = \mathcal{G}_i(a) \frac{\partial f^t}{\partial x}(a) e^t = 0.$$

To this end, note that $\mathcal{G}_i f^t \in M_{l \times 1}(\mathbb{F}_q[x_1, \dots, x_n])$ consists of the entries of G_{-i} , arranged in a column. Therefore

$$\mathcal{G}_i(a) \frac{\partial f^t}{\partial x}(a) = \frac{\partial(\mathcal{G}_i f^t)}{\partial x}(a) = \frac{\partial G_{-i}}{\partial x}(a) = \begin{pmatrix} 0 & \frac{\partial G_{-i}}{\partial x_{-i}}(a) \end{pmatrix} = \begin{pmatrix} 0 & \mathcal{G}_i(a) \frac{\partial f^t}{\partial x_{-i}}(a) \end{pmatrix},$$

according to $f^t(a) = 0_{m \times 1}$, whereas

$$\mathcal{G}_i(a) \frac{\partial f^t}{\partial x}(a) e^t = \mathcal{G}_i(a) \frac{\partial f^t}{\partial x_{-i}}(a) \Pi_i(e)^t.$$

Any $e \in \mathbb{F}_{q^{\delta(a)}}^n$ with $\text{Supp}(e) \subseteq i$ has $\Pi_i(e) = 0^{n-t}$, so that $\mathcal{G}_i(a) \frac{\partial f^t}{\partial x}(a) e^t = 0$. Conversely, if

$$0 = \mathcal{G}_i(a) \frac{\partial f^t}{\partial x}(a) e^t = \frac{\partial G_{-i}}{\partial x_{-i}}(a) \Pi_i(e)^t$$

for some $e = (\Pi_{-i}(e), \Pi_i(e)) \in \mathbb{F}_{q^{\delta(a)}}^n$ then $\Pi_i(e) \in T_{\Pi_i(a)}(\overline{\Pi_i(X)}, \mathbb{F}_{q^{\delta(a)}})$. By the surjectiveness of (2), there exists $v_o = (\Pi_{-i}(v_o), \Pi_i(e)) \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$. Now,

$$e_o := e - v_o = (\Pi_{-i}(e - v_o), 0)$$

has $\text{Supp}(e_o) \subseteq i$ and $w - e_o = w - e + v_o \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$.

The polynomials $h = \{h_1, \dots, h_l\} = G_{-i} \subset \mathbb{F}_q[x_{-i}]$ have Jacobian matrix

$$\frac{\partial h}{\partial x}(a) = \frac{\partial G_{-i}}{\partial x}(a) = \frac{\partial}{\partial x} (\mathcal{G}_i(x) f^t(x)) (a) = \mathcal{G}_i(a) \frac{\partial f}{\partial x}(a)$$

at $a \in X$. As a result, $w \in \mathbb{F}_{q^{\delta(a)}}^n$ has a $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error, supported by i exactly when $\frac{\partial h}{\partial x}(a) w^t = 0_{l \times 1}$. By Lemma 6 (ii), the absolute ideal $I(\Pi_i(X), \overline{\mathbb{F}_q}) = I(\overline{\Pi_i(X)}, \overline{\mathbb{F}_q}) = \langle G_{-i} \rangle_{\overline{\mathbb{F}_q}} = \langle h_1, \dots, h_l \rangle_{\overline{\mathbb{F}_q}}$ of $\Pi_i(X)$ is generated by $h_1, \dots, h_l \in \mathbb{F}_q[x_1, \dots, x_n]$. The absolute ideal of the cylinder $\Pi_i^{-1}(\overline{\Pi_i(X)})$ is the extension

$$I(\Pi_i^{-1}(\overline{\Pi_i(X)})) = I(\overline{\Pi_i(X)}, \overline{\mathbb{F}_q}) \otimes_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q}[x_1, \dots, x_n]$$

of $I(\overline{\Pi_i(X)}, \overline{\mathbb{F}_q})$ to an ideal of $\overline{\mathbb{F}_q}[x_1, \dots, x_n]$. Therefore, the Zariski tangent space to $\Pi_i^{-1}(\overline{\Pi_i(X)})$ at $a \in X \subseteq \Pi_i^{-1}(\overline{\Pi_i(X)})$ is

$$T_a(\Pi_i^{-1}(\overline{\Pi_i(X)}), \mathbb{F}_{q^{\delta(a)}}) = \left\{ w \in \mathbb{F}_{q^{\delta(a)}}^n \mid \frac{\partial G_{-i}}{\partial x}(a) w^t = \frac{\partial h}{\partial x}(a) w^t = 0_{|G_{-i}| \times 1} \right\}.$$

In such a way we have established that there is $e \in \mathbb{F}_{q^{\delta(a)}}^n$ with $\text{Supp}(e) \subseteq i$ and $w - e \in T_a(X, \mathbb{F}_{q^{\delta(a)}})$ if and only if $w \in T_a(\Pi_i^{-1}(\overline{\Pi_i(X)}), \mathbb{F}_{q^{\delta(a)}})$. Making use of $\frac{\partial f}{\partial x}(a)(w^t - e^t) = 0_{m \times 1}$ and $\Pi_i(e) = 0^{n-t}$, one concludes that

$$\frac{\partial f}{\partial x_i}(a)e_i^t = \frac{\partial f}{\partial x}(a)e^t = \frac{\partial f}{\partial x}(a)w^t.$$

□

Note that Proposition 7 can be used for computing the leaders of those cosets $w + T_a(X, \mathbb{F}_{q^{\delta(a)}}) \in \mathbb{F}_{q^{\delta(a)}}^n / T_a(X, \mathbb{F}_{q^{\delta(a)}})$, which admit representatives of weight less than the minimum distance of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$.

Here is an algorithm for simultaneous decoding of tangent codes.

Corollary 8. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, whose absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ is generated by $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ and*

$$\pi : \text{Err}(TX, t) := \coprod_{a \in X^{(\geq 2t+1)}} \text{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), t) \longrightarrow X^{(\geq 2t+1)}$$

be the bundle of the words with TX -error of weight $\leq t$. Then any $w \in \text{Err}(TX, t)$ can be decoded by the following algorithm:

Step 1: *For any $i \in \Sigma_t(1, \dots, n)$ apply Buchberger's algorithm and obtain a Groebner basis $G_{i \neg i}$ of $I(X, \mathbb{F}_q) = \langle f_1, \dots, f_m \rangle_{\mathbb{F}_q}$ with respect to a lexicographic order of $\mathbb{F}_q[x_1, \dots, x_n]$ with $x_i >_{\text{lex}} x_{\neg i}$. Single out the polynomials $G_{\neg i} := G_{i \neg i} \cap \mathbb{F}_q[x_{\neg i}]$ from $G_{i \neg i}$, which do not depend on x_{i_1}, \dots, x_{i_t} for $i = \{i_1, \dots, i_t\}$.*

Step 2: *For arbitrary*

$$i, j \in \Sigma_t(1, \dots, n)$$

compute the determinant

$$\Delta_{ji} := \det \frac{\partial f_j}{\partial x_i} \in \mathbb{F}_q[x_1, \dots, x_n],$$

the inverse matrix

$$\left(\frac{\partial f_j}{\partial x_i} \right)^{-1} \in M_{t \times t}(\Delta_{ji}^{-1} \mathbb{F}_q[x_1, \dots, x_n])$$

and the product

$$\left(\frac{\partial f_j}{\partial x_i} \right)^{-1} \frac{\partial f_j}{\partial x} \in M_{t \times n} \left(\Delta_{ji}^{-1} \mathbb{F}_q[x_1, \dots, x_n] \right).$$

Step 3: *If $w \in \text{Err}(TX, t)$ and $\pi(w) = a \in X^{(\leq 2t+1)}$ then compute the products*

$$\frac{\partial G_{\neg \gamma}}{\partial x_{\neg \gamma}}(a)w^t \quad \text{for } \gamma \in \Sigma_t(1, \dots, n)$$

until you recognize the unique $i \in \Sigma_t(1, \dots, n)$ with

$$\frac{\partial G_{\neg i}}{\partial x_{\neg i}}(a)w^t = 0_{|G_{\neg i}| \times 1}.$$

Step 4: Plug in a in $\Delta_{ji} \in \mathbb{F}_q[x_1, \dots, x_n]$ and choose some $j \in \Sigma_t(1, \dots, n)$ with $\Delta_{ji}(a) \neq 0$. (For any $i \in \Sigma_t(1, \dots, n)$ and $a \in X$, subject to the aforementioned properties, there exists at least one $j \in \Sigma_t(1, \dots, n)$ with $\Delta_{ji}(a) \neq 0$.)

Step 5: The unique $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ -error

$$e = (\Pi_{-i}(e), \Pi_i(e)) = (\Pi_{-i}(e), 0_{1 \times (n-t)}) \in \mathbb{F}_{q^{\delta(a)}}^n$$

of $w \in \text{Err}(T_a(X, \mathbb{F}_{q^{\delta(a)}}), t) \subset \mathbb{F}_{q^{\delta(a)}}^n$ has projection

$$\Pi_{-i}(e) = (e_{i_1}, \dots, e_{i_t}) = e_i := \left[\left(\frac{\partial f_j}{\partial x_i} \right)^{-1} \frac{\partial f_j}{\partial x} \right] (a) w^t \in \mathbb{F}_{q^{\delta(a)}}^t$$

onto the components, labeled by i .

4.2 Lower semi-continuity of the generic minimum distance

If $X \subseteq \overline{\mathbb{F}_q}^n$ is an affine variety with absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ then $k = \dim X \geq n - m$, as far as any polynomial relation f_j on X decreases the dimension at most by 1. If $I(X, \overline{\mathbb{F}_q})$ admits a generating set with minimal cardinality $m = n - k$, then X is called a complete intersection.

Suppose that the generators f_j of $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_{n-k} \rangle_{\overline{\mathbb{F}_q}}$ are of the form $f_j = \sum_{\nu \in (\mathbb{Z}^{\geq 0})^n} \alpha_{j,\nu} x^\nu \in \mathbb{F}_q[x]$, where $x^\nu := x_1^{\nu_1} \dots x_n^{\nu_n}$. The set

$$S(f_j) := \{ \nu \in (\mathbb{Z}^{\geq 0})^n \setminus \{0^n\} \mid \alpha_{j,\nu} \neq 0 \}$$

will be referred to as the non-constant support of f_j . For an arbitrary smooth point $a \in X^{\text{smooth}}$ let

$$F_j(y_j, x) := \sum_{\nu \in S(f_j)} y_{j,\nu} (x^\nu - a^\nu) \in \mathbb{F}_{q^{\delta(a)}}[x, y_j]$$

and note that $F_j(y_j, a) \equiv 0 \in \mathbb{F}_{q^{\delta(a)}}[y_j] = \mathbb{F}_{q^{\delta(a)}}[y_{j,\nu} \mid \nu \in S(f_j)]$. The maps $S(f_j) \rightarrow \overline{\mathbb{F}_q}$ are in a bijective correspondence with the collections $\gamma_j = \{ \gamma_{j,\nu} \in \overline{\mathbb{F}_q} \mid \nu \in S(f_j) \}$ of their images. That is why the set $\overline{\mathbb{F}_q}^{S(f_j)}$ of the maps $S(f_j) \rightarrow \overline{\mathbb{F}_q}$ can be identified with the affine space of dimension $|S(f_j)|$ over $\overline{\mathbb{F}_q}$. The product

$$\mathcal{A} = \mathcal{A}(f, a) := \overline{\mathbb{F}_q}^{S(f_1)} \times \dots \times \overline{\mathbb{F}_q}^{S(f_{n-k})}$$

parameterizes the polynomials $F(\gamma, x) = \{F_1(\gamma_1, x), \dots, F_m(\gamma_{n-k}, x)\}$ and the affine varieties $X_\gamma := V(F(\gamma, x)) = V(F_1(\gamma_1, x), \dots, F_{n-k}(\gamma_{n-k}, x)) \subset \overline{\mathbb{F}_q}^n$ through a . We are going to show that $\dim X_\gamma = \dim X = k$ for "almost all" $\gamma \in \mathcal{A}$ and the minimum distance $d(T_a(X_\gamma, \mathbb{F}_{q^{\delta(a)}})) \geq d$ at "almost all" the points of $\{(\gamma, a) \in \mathcal{A} \times \overline{\mathbb{F}_q}^n \mid a \in X_\gamma\}$.

For an arbitrary polynomial

$$g(y, x) \in \mathbb{F}_{q^{\delta(a)}}[y, x] = \mathbb{F}_{q^{\delta(a)}}[x_1, \dots, x_n, y_{j,\nu_j} \mid \nu_j \in S(f_j), 1 \leq j \leq n - k],$$

let us denote by $\mathcal{W}_{\mathcal{A}}(g(y, a)) := \{\gamma \in \mathcal{A} \mid g(\gamma, a) = 0\} \subseteq \mathcal{A}$ the hypersurface, cut by the polynomial $g(y, a) \in \mathbb{F}_{q^{\delta(a)}}[y_j, \nu_j \mid \nu_j \in S(f_j), 1 \leq j \leq n-k]$ for some $a \in \overline{\mathbb{F}_q}^n$. Note also that for any $\gamma \in \mathcal{A}$ the polynomial $g(\gamma, x) \in \mathbb{F}_{q^{\delta(\gamma, a)}}[x_1, \dots, x_n]$ determines a hypersurface $V(g(\gamma, x)) := \{b \in \overline{\mathbb{F}_q}^n \mid g(\gamma, b) = 0\} \subseteq \overline{\mathbb{F}_q}^n$.

Proposition 9. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be a complete intersection, defined over \mathbb{F}_q and $a \in X^{\text{smooth}}$ be a smooth point of X , at which the Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ is of minimum distance $d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) \geq d$. Then there exist non-zero polynomials $g(y, x), h(y, x) \in \mathbb{F}_{q^{\delta(a)}}[y, x] \setminus \{0\}$, such that $\dim X_\gamma = \dim X$, $a \in X_\gamma^{\text{smooth}}$ and*

$$\emptyset \neq X_\gamma \setminus V(g(\gamma, x)) \subseteq X_\gamma^{(\geq d)} \quad \text{for all } \gamma \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(g(y, a)h(y, a))$$

Proof. Let $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_{n-k} \rangle_{\overline{\mathbb{F}_q}}$ for some $f_1, \dots, f_{n-k} \in \mathbb{F}_q[x_1, \dots, x_n]$ and $F_j(y_j, x) := \sum_{\nu \in S(f_j)} y_{j, \nu} (x^\nu - a^\nu) \in \mathbb{F}_{q^{\delta(a)}}[x, y_j]$ for the non-constant supports $S(f_j) \subset (\mathbb{Z}^{\geq 0})^n \setminus \{0^n\}$ of f_j with $1 \leq j \leq n-k$. By its very definition, the affine variety $X_\alpha := V(F_1(\alpha, x), \dots, F_{n-k}(\alpha, x))$ coincides with X . The point $a \in X_\alpha$ is smooth exactly when the Jacobian matrix $\frac{\partial(F_1(\alpha, x), \dots, F_{n-k}(\alpha, x))}{\partial x}$ is of maximal rank $\text{rk} \frac{\partial F(\alpha, x)}{\partial x}(a) = n-k$ at a . That implies the existence of $j \in \Sigma_{n-k}(1, \dots, n)$ with $\det \frac{\partial F(\alpha, x)}{\partial x_j}(a) \neq 0$. The polynomial

$$h(y, x) := \det \frac{\partial F(y, x)}{\partial x_j} \in \mathbb{F}_{q^{\delta(a)}}[y, x]$$

cuts a proper hypersurface $\mathcal{W}_{\mathcal{A}}(h(y, a)) \subsetneq \mathcal{A}$, as far as $\alpha \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(h(y, a))$. By the very construction, $a \in X_\gamma$ for all $\gamma \in \mathcal{A}$. Note that an arbitrary affine variety $X_\gamma = V(F_1(\gamma, x), \dots, F_{n-k}(\gamma, x))$ is of dimension $\dim X_\gamma \geq k$. According to $\dim T_a(X_\gamma, \mathbb{F}_{q^{\delta(\gamma, a)}}) \geq \dim X_\gamma$, it suffices to show that $\dim T_a(X_\gamma, \mathbb{F}_{q^{\delta(\gamma, a)}}) \leq k$ for $\forall \gamma \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(h(y, a))$ in order to conclude that $\dim X_\gamma = k$ and $a \in X_\gamma^{\text{smooth}}$ is a smooth point of X_γ for all $\gamma \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(h(y, a))$. Indeed, $\gamma \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(h(y, a))$ amounts to

$$\left(\det \frac{\partial F(\gamma, x)}{\partial x_j} \right) (a) = h(\gamma, a) \neq 0.$$

According to $F_1(\gamma, x), \dots, F_{n-k}(\gamma, x) \in I(X_\gamma, \overline{\mathbb{F}_q})$, the tangent code $T_a(X_\gamma, \mathbb{F}_{q^{\delta(\gamma, a)}})$ is contained in the $\mathbb{F}_{q^{\delta(\gamma, a)}}$ -linear code $C_{\gamma, a}$ with parity check matrix $\frac{\partial F(\gamma, x)}{\partial x}(a) \in M_{(n-k) \times n}(\mathbb{F}_{q^{\delta(\gamma, a)}})$. Bearing in mind that $n-k \geq \text{rk} \frac{\partial F(\gamma, x)}{\partial x}(a) \geq \text{rk} \frac{\partial F(\gamma, x)}{\partial x_j}(a) = n-k$, one concludes that $\dim C_{\gamma, a} = k$ and

$$\dim T_a(X_\gamma, \mathbb{F}_{q^{\delta(\gamma, a)}}) \leq \dim C_{\gamma, a} = k.$$

Thus, $\dim X_\gamma = k$ for all $\gamma \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(h(y, a))$.

It suffices to construct a polynomial $g(y, x) \in \mathbb{F}_{q^{\delta(a)}}[y, x]$ with $g(a, a) \neq 0$, such that for any $\gamma \in \mathcal{A}$ the points $b \in X_\gamma$ with $d(T_b(X_\gamma, \mathbb{F}_{q^{\delta(\gamma, a, b)}})) < d$ belong to the hypersurface $V(g(\gamma, x)) \subset \overline{\mathbb{F}_q}^n$. Then $\mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(g(y, a)h(y, a)) \ni \alpha$ is non-empty and $X_\gamma \setminus V(g(\gamma, x)) \ni a$ is non-empty for any $\gamma \in \mathcal{A} \setminus \mathcal{W}_{\mathcal{A}}(g(y, a)h(y, a))$. Moreover,

$d(T_b(X_\gamma, \mathbb{F}_{q^{\delta(\gamma, a, b)}})) \geq d$ for any $\gamma \in \mathcal{A} \setminus \mathcal{W}_\mathcal{A}(g(y, a)h(y, a))$ and $b \in X_\gamma \setminus V(g(\gamma, x))$. Towards the construction of $g(y, x) \in \mathbb{F}_{q^{\delta(a)}}[y, x]$ with the desired properties, note that

$$X_\gamma^{(<d)} \subseteq Z_{\gamma, d} := \cup_{i \in \Sigma_{d-1}(1, \dots, n)} V \left(\det \frac{\partial F_\sigma(\gamma_\sigma, x)}{\partial x_i} \mid \sigma \in \Sigma_{d-1}(1, \dots, n-k) \right),$$

according to $F_1(\gamma_1, x), \dots, F_{n-k}(\gamma_{n-k}, x) \in I(X_\gamma, \overline{\mathbb{F}_q})$. In particular, the point a does not belong to $X_\alpha^{(<d)} = Z_{\alpha, d}$ and for any $i \in \Sigma_{d-1}(1, \dots, n)$ there exists $\rho(i) \in \Sigma_{d-1}(1, \dots, n-k)$ with $\det \frac{\partial F_{\rho(i)}(\alpha_{\rho(i)}, x)}{\partial x_i}(a) \neq 0$. As a result,

$$a \notin \cup_{i \in \Sigma_{d-1}(1, \dots, n)} V \left(\det \frac{\partial F_{\rho(i)}(\alpha_{\rho(i)}, x)}{\partial x_i} \right) = V \left(\prod_{i \in \Sigma_{d-1}(1, \dots, n)} \det \frac{\partial F_{\rho(i)}(\alpha_{\rho(i)}, x)}{\partial x_i} \right).$$

If

$$g(y, x) := \prod_{i \in \Sigma_{d-1}(1, \dots, n)} \det \frac{\partial F_{\rho(i)}(y_{\rho(i)}, x)}{\partial x_i} \in \mathbb{F}_{q^{\delta(a)}}[y, x]$$

then $g(\alpha, a) \neq 0$. Straightforwardly,

$$\begin{aligned} X_\gamma^{(<d)} &:= \{b \in X_\gamma \mid d(T_b(X_\gamma, \mathbb{F}_{q^{\delta(b)}})) < d\} \subseteq \\ Z_{\gamma, d} &:= \cup_{i \in \Sigma_{d-1}(1, \dots, n)} V \left(\det \frac{\partial F_\sigma(\gamma_\sigma, x)}{\partial x_i} \mid \sigma \in \Sigma_{d-1}(1, \dots, n-k) \right) \subseteq \\ &\cup_{i \in \Sigma_{d-1}(1, \dots, n)} V \left(\det \frac{\partial F_{\rho(i)}(\gamma_{\rho(i)}, x)}{\partial x_i} \right) = V(g(\gamma, x)). \end{aligned}$$

□

4.3 Gradient codes

Let $X \subset \overline{\mathbb{F}_q}^n$ be an affine variety, whose absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ is generated by $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$. For an arbitrary constant field $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}_q}$, the Zariski tangent bundle of X over F is defined as the disjoint union

$$T(X, F) := \coprod_{a \in X(F)} T_a(X, F)$$

of the Zariski tangent spaces to X over F at the F -rational points $a \in X(F) := X \cap F^n$. Note that the fibres of $T(X, F)$ are not supposed to be of one and a same dimension over F . The union

$$T(X, F)^\perp := \coprod_{a \in X(F)} T_a(X, F)^\perp$$

of the dual codes $T_a(X, F)^\perp$ of $T_a(X, F)$ is referred to as the dual of the Zariski tangent bundle to X over F .

As far as the absolute ideal

$$I(X, \overline{\mathbb{F}_q}) := \{g \in \overline{\mathbb{F}_q}[x_1, \dots, x_n] \mid g(a) = 0, \forall a \in X\}$$

of X is generated by polynomials $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ with coefficients from \mathbb{F}_q , for an arbitrary constant field $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}_q}$ the ideal

$$I(X, F) := \{g \in F[x_1, \dots, x_n] \mid g(a) = 0, \forall a \in X\}$$

of X over F is generated by $f_1, \dots, f_m \in F[x_1, \dots, x_n]$, i.e., $I(X, F) = \langle f_1, \dots, f_m \rangle_F$. For any $g \in I(X, F)$ the ordered n -tuple of polynomials

$$\text{grad}(g) := \left(\frac{\partial g}{\partial x_1}, \dots, \frac{\partial g}{\partial x_n} \right) \in F[x_1, \dots, x_n]^n$$

is called the gradient of g . We consider the F -linear space

$$\text{Grad}I(X, F) := \{\text{grad}(g) \mid g \in I(X, F)\} \subset F[x_1, \dots, x_n]^n$$

of the gradients of the polynomials from $I(X, F)$ and its evaluations

$$\text{grad}_a I(X, F) := \{\text{grad}(g)(a) \mid g \in I(X, F)\} \subseteq F^n$$

at the F -rational points $a \in X(F) := X \cap F^n$ of X . That allows to form the vector bundle

$$\text{grad}I(X, F) = \coprod_{a \in X(F)} \text{grad}_a I(X, F) \subset X(F) \times F^n$$

over $X(F)$, contained in the trivial bundle $X(F) \times F^n$. The fibres $\text{grad}_a I(X, F)$ of $\text{grad}I(X, F)$ are not supposed to be of one and a same dimension. Nevertheless, we say that

$$\text{grad}I(X, F) \longrightarrow X(F)$$

the gradient bundle of X (or of $I(X, F)$) over F .

Lemma 10. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an affine variety with $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ for some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ and $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}_q}$ be a constant field. Then the dual*

$$T(X, F)^\perp = \text{grad}I(X, F) \tag{3}$$

of the Zariski tangent bundle $T(X, F)$ of X over F is the gradient bundle of X (or of $I(X, F)$) over $X(F)$.

Proof. The equality (3) is meant as a coincidence $T_a(X, F)^\perp = \text{grad}_a I(X, F)$ of the fibres over all the points $a \in X(F)$. By its very definition, $T_a(X, F)^\perp$ is the linear code with a generator matrix

$$\frac{\partial f}{\partial x}(a) = \begin{pmatrix} \text{grad}(f_1)(a) \\ \vdots \\ \text{grad}(f_m)(a) \end{pmatrix}.$$

Therefore

$$T_a(X, F)^\perp = \left\{ \sum_{j=1}^m \lambda_j \text{grad}(f_j)(a) = \text{grad} \left(\sum_{j=1}^m \lambda_j f_j \right) (a) \mid \lambda_j \in F \right\}$$

is a subspace of $\text{grad}_a I(X, F)$, as far as $\sum_{j=1}^m \lambda_j f_j \in I(X, F)$ for $\forall \lambda_j \in F$. Conversely, any element of $I(X, F)$ is of the form $g = \sum_{j=1}^m g_j f_j$ for some $g_j \in F[x_1, \dots, x_n]$. Then $\text{grad}(g) = \sum_{j=1}^m f_j \text{grad}(g_j) + g_j \text{grad}(f_j)$ and

$$\begin{aligned} \text{grad}(g)(a) &= \sum_{j=1}^m g_j(a) \text{grad}(f_j)(a) \in \text{Span}_F(\text{grad}(f_1)(a), \dots, \text{grad}(f_m)(a)) \\ &= T_a(X, F)^\perp. \end{aligned}$$

Thus, $\text{grad}_a I(X, F) \subseteq T_a(X, F)^\perp$ and $T_a(X, F)^\perp = \text{grad}_a I(X, F)$. □

Note that

$$\text{Grad}I(X, F) := \{\text{grad}(g) \mid g \in I(X, F)\} \subset F[x_1, \dots, x_n]^n$$

and

$$\begin{aligned} \overline{\text{Grad}}I(X, F) &:= \left\{ \left(\frac{\partial g}{\partial x_1} + I(X, F), \dots, \frac{\partial g}{\partial x_n} + I(X, F) \right) \mid g \in I(X, F) \right\} \subset \\ &\quad [F[x_1, \dots, x_n]/I(X, F)]^n = F[X]^n \end{aligned}$$

can be viewed as sheaves of sections of $\text{grad}I(X, F) = T(X, F)^\perp \rightarrow X(F)$. Thus, the gradient codes consist of values of global sections of vector bundles and appear to be of a similar nature with Goppa codes. In order to specify, let $Y/\mathbb{F}_q \subset \mathbb{P}^N(\overline{\mathbb{F}}_q)$ be a smooth irreducible projective curve, defined over \mathbb{F}_q , $D = P_1 + \dots + P_n$ be a sum of n different \mathbb{F}_q -rational points $P_1, \dots, P_n \in X(\mathbb{F}_q)$ and G be a divisor on Y with $\text{Supp}(G) \cap \text{Supp}(D) = \emptyset$. Denote by $\mathcal{O}_Y([G]) \rightarrow Y$ the line bundle, associated with G and consider the evaluation map

$$\mathcal{E}_D : H^0(Y, \mathcal{O}_Y([G])) \longrightarrow \mathbb{F}_q^n,$$

$$\mathcal{E}_D(s) := (s(P_1), \dots, s(P_n))$$

of the global sections $s \in H^0(Y, \mathcal{O}_Y([G]))$ of $\mathcal{O}_Y([G])$. The image $\mathcal{E}_D H^0(Y, \mathcal{O}_Y([G]))$ of \mathcal{E}_D is called a Goppa code. It consists of the values $(s(P_1), \dots, s(P_n))$ of the global sections $s \in H^0(Y, \mathcal{O}_Y([G]))$ of the line bundle $\mathcal{O}_Y([G]) \rightarrow Y$ at the ordered n -tuple of points (P_1, \dots, P_n) , while $\text{grad}_a I(X, F)$ is constituted by the values

$$\text{grad}(g)(a) = \left(\frac{\partial g}{\partial x_1}, \dots, \frac{\partial g}{\partial x_n} \right) (a) = \left(\frac{\partial g}{\partial x_1} + I(X, F), \dots, \frac{\partial g}{\partial x_n} + I(X, F) \right) (a)$$

of the global sections

$$\text{grad}(g) = \left(\frac{\partial g}{\partial x_1}, \dots, \frac{\partial g}{\partial x_n} \right) \quad \text{or} \quad \left(\frac{\partial g}{\partial x_1} + I(X, F), \dots, \frac{\partial g}{\partial x_n} + I(X, F) \right)$$

of $\text{grad}I(X, F) \rightarrow X(F)$.

For an arbitrary integer $0 \leq s \leq n$, let us consider the loci

$$\begin{aligned} X_{\text{grad}}^{(\geq s)} &:= \{a \in X \mid d(\text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})) \geq s\}, \\ X_{\text{grad}}^{(\leq s)} &:= \{a \in X \mid d(\text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})) \leq s\}, \end{aligned}$$

at which the gradient codes to X are of minimum distance $\geq s$, respectively, $\leq s$. The next proposition shows that the presence of a non-zero polynomial from $I(X, \overline{\mathbb{F}_q})$ in d variables imposes an upper bound d on the minimum distance of a gradient code to X at "almost all" the points of X .

Proposition 11. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over \mathbb{F}_q , for which there exists a non-zero polynomial $h \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\beta]$ of $|\beta| = d$ variables and $\Pi_{\neg\beta} : X \rightarrow \overline{\mathbb{F}_q}^d$ be the puncturing at the complement $\neg\beta$ of β . Then*

$$X_{\text{grad}}^{(\geq d+1)} \subseteq \Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}}) \subsetneq X,$$

so that $X_{\text{grad}}^{(\leq d)}$ is Zariski dense in X .

Proof. By assumption, $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ is generated by some polynomials $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$. Let $G_{\neg\beta, \beta} \subset \mathbb{F}_q[x_1, \dots, x_n]$ be a Groebner basis of $\langle f_1, \dots, f_m \rangle_{\mathbb{F}_q}$ with respect to a lexicographic order with $x_{\neg\beta} >_{\text{lex}} x_\beta$ and

$$G_\beta := G_{\neg\beta, \beta} \cap \mathbb{F}_q[x_\beta] = \{h_1, \dots, h_l\}.$$

As in the proof of Proposition 7, $h_1, \dots, h_l \in \mathbb{F}_q[x_1, \dots, x_n]$ generate the absolute ideal

$$I(\overline{\Pi_{\neg\beta}(X)}, \overline{\mathbb{F}_q}) = I(\Pi_{\neg\beta}(X), \overline{\mathbb{F}_q}) = I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\beta] = \langle G_\beta \rangle_{\overline{\mathbb{F}_q}} = \langle h_1, \dots, h_l \rangle_{\overline{\mathbb{F}_q}}$$

of $\Pi_{\neg\beta}(X)$. By the Elimination Theorem 2 from Chapter 2, §1, [3], G_β is a Groebner basis of $I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\beta] \triangleleft \overline{\mathbb{F}_q}[x_\beta]$, so that the presence of a non-zero polynomial $h \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\beta]$ implies that the set $G_\beta \neq \emptyset$ is non-empty. As a result, $\overline{\Pi_{\neg\beta}(X)} \subsetneq \overline{\mathbb{F}_q}^d$ is an irreducible affine variety of dimension $\dim \Pi_{\neg\beta}(X) < d$.

For any $h_i \in I(\Pi_{\neg\beta}(X), \mathbb{F}_{q^{\delta(a)}}) \subseteq I(X, \mathbb{F}_{q^{\delta(a)}})$ and $a \in X$ note that $\text{grad}(h_i)(a) \in \text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})$ is a word of weight $\leq d$, as far as $h_i \in \mathbb{F}_{q^{\delta(a)}}[x_\beta]$ depends on at most $|\beta| = d$ variables. In particular, for $a \in X_{\text{grad}}^{(\geq d+1)}$ there follows $\text{grad}(h_i)(\Pi_{\neg\beta}(a)) = \text{grad}(h_i)(a) = 0$. Thus,

$$\frac{\partial(h_1, \dots, h_l)}{\partial x_\beta}(\Pi_{\neg\beta}(a)) = \begin{pmatrix} \text{grad}(h_1) \\ \dots \\ \text{grad}(h_l) \end{pmatrix}(\Pi_{\neg\beta}(a)) = 0 \quad \text{at} \quad \forall a \in X_{\text{grad}}^{(\geq d+1)}$$

and

$$X_{\text{grad}}^{(\geq d+1)} \subseteq V\left(\frac{\partial h_i}{\partial x_j} \mid 1 \leq i \leq l, \ 1 \leq j \leq n\right).$$

We claim that

$$V\left(\frac{\partial h_i}{\partial x_j} \mid 1 \leq i \leq l, 1 \leq j \leq n\right) \subseteq \Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}}).$$

Indeed, if $\frac{\partial h_i}{\partial x_j}(a) = 0$ for $\forall 1 \leq i \leq l, \forall 1 \leq j \leq n$ then

$$T_{\Pi_{\neg\beta}(a)}(\Pi_{\neg\beta}(X), \mathbb{F}_{q^{\delta(a)}}) = \mathbb{F}_{q^{\delta(a)}}.$$

According to $\dim \Pi_{\neg\beta}(X) < d$ there follows $\Pi_{\neg\beta}(a) \in \Pi_{\neg\beta}(X)^{\text{sing}}$, which is equivalent to $a \in \Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}})$. Thus,

$$X_{\text{grad}}^{(\geq d+1)} \subseteq V\left(\frac{\partial h_i}{\partial x_j} \mid 1 \leq i \leq l, 1 \leq j \leq n\right) \subseteq \Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}}).$$

The assumption $\Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}}) = X$ leads to $\Pi_{\neg\beta}(X) = \Pi_{\neg\beta}(X)^{\text{sing}}$ and contradicts $\Pi_{\neg\beta}(X)^{\text{smooth}} \neq \emptyset$.

Note that $X_{\text{grad}}^{(\geq d+1)} \subseteq \Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}})$ implies

$$\Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{smooth}}) = X \setminus \Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{sing}}) \subseteq X \setminus X_{\text{grad}}^{(\geq d+1)} = X_{\text{grad}}^{(\leq d)}.$$

The non-empty subset $\Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{smooth}}) \subseteq X$ is Zariski open, as far as the smooth locus $\Pi_{\neg\beta}(X)^{\text{smooth}}$ is an open subset of $\Pi_{\neg\beta}(X)$ and $\Pi_{\neg\beta}$ is continuous with respect to the Zariski topology. Therefore $\Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{smooth}})$ is Zariski dense in the irreducible affine variety X and the Zariski closure $\overline{X_{\text{grad}}^{(\leq d)}}$ of $X_{\text{grad}}^{(\leq d)}$ coincides with X , according to

$$X = \overline{\Pi_{\neg\beta}^{-1}(\Pi_{\neg\beta}(X)^{\text{smooth}})} \subseteq \overline{X_{\text{grad}}^{(\leq d)}} \subseteq X.$$

□

Note that $X_{\text{grad}}^{(d)}$ is not claimed to be Zariski open in X . If there exists a polynomial global tangent frame on X then there is a polynomial family of parity check matrices of the gradient codes to X and $X_{\text{grad}}^{(d)}$ is Zariski closed in X . As a result, $X = X_{\text{grad}}^{(d)}$ and $\Pi_{\neg\beta}(X) \subset \overline{\mathbb{F}_q^d}$ is smooth.

5 Tangent codes of special type

5.1 Near MDS tangent and gradient codes

According to Proposition 2 (i), if an irreducible affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q^d}$, defined over \mathbb{F}_q has at least one MDS tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ then the locus

$$X^{(n-k+1)} := \{a \in X \mid d(T_a(X, \mathbb{F}_{q^{\delta(a)}})) = n - k + 1\}$$

of the MDS tangent codes to X is Zariski open and Zariski dense in X .

The present subsection is devoted to the near MDS-codes, introduced by Dudenkov and Landgev in [4]. These can be defined as the linear codes $C \subset \mathbb{F}_q^n$ of $\dim C = k$ and minimum distance $d(C) = n - k$, whose duals $C^\perp \subset \mathbb{F}_q^n$ are of minimum distance $d(C^\perp) = k$. If $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ is an irreducible k -dimensional affine variety, defined over \mathbb{F}_q and X^{NMDS} is the set of the points $a \in X$, at which the tangent code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ is near MDS then $X^{\text{NMDS}} \subseteq X^{(n-k)}$. We show that X^{NMDS} is a Zariski open subset of X . If $X^{\text{NMDS}} \neq \emptyset$ is non-empty, then X^{NMDS} is Zariski dense in $X^{(n-k)}$ and in X .

In the statement and the proof of the next proposition we abbreviate $\Sigma_s(n) := \Sigma_s(1, \dots, n)$, respectively, $\Sigma_r(m) := \Sigma_r(1, \dots, m)$, in order to simplify the notation.

Proposition 12. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible k -dimensional affine variety with $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ for some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ and $\Pi_\alpha : X \rightarrow \Pi_\alpha(X)$ be a non-finite puncturing at $|\alpha| = n - k$ coordinates. Then the subset $X^{\text{NMDS}} \subseteq X$ of the points $a \in X$ at which $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ is a near MDS code is Zariski open,*

$$X^{\text{NMDS}} = X^{(n-k)} \setminus V \left(\prod_{\beta \in \Sigma_{n-k+1}(n)} \det \frac{\partial f_{\psi(\beta)}}{\partial x_{\theta(\beta)}} \mid \begin{array}{l} \psi : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(m), \\ \theta : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(n) \\ \theta(\beta) \in \Sigma_{n-k}(\beta) \end{array} \right) =$$

$$X \setminus V \left(\prod_{i \in \Sigma_{n-k-1}(n)} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \prod_{\beta \in \Sigma_{n-k+1}(n)} \det \frac{\partial f_{\psi(\beta)}}{\partial x_{\theta(\beta)}} \mid \begin{array}{l} \varphi : \Sigma_{n-k-1}(n) \rightarrow \Sigma_{n-k-1}(m), \\ \psi : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(m), \\ \theta : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(n), \\ \theta(\beta) \in \Sigma_{n-k}(\beta) \end{array} \right) \quad \blacksquare$$

both in $X^{(n-k)}$ and in X . Thus, if some Zariski tangent space $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ at a smooth point $a \in X$ is a near MDS-code then X^{NMDS} is Zariski dense in $X^{(n-k)}$, X and $I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\gamma] = \{0\}$ for $\forall \gamma \in \Sigma_{k-1}(n)$.

Proof. By Lemma 3.1 from [4], an $[n, k, n - k]_q$ -code $T_a(X, \mathbb{F}_{q^{\delta(a)}})$ with a parity check matrix $\frac{\partial f}{\partial x}(a)$ is near MDS exactly when for $\forall \beta \in \Sigma_{n-k+1}(n)$ the matrix $\frac{\partial f}{\partial x_\beta}(a) \in M_{m \times (n-k+1)}(\mathbb{F}_{q^{\delta(a)}})$ is of maximal rank $\text{rk} \frac{\partial f}{\partial x_\beta}(a) = n - k$. Thus,

$$X^{(n-k)} \setminus X^{\text{NMDS}} = X^{(n-k)} \cap \left[\bigcup_{\beta \in \Sigma_{n-k+1}(n)} \left\{ a \in X \mid \text{rk} \frac{\partial f}{\partial x_\beta}(a) < n - k \right\} \right].$$

The minors of $\frac{\partial f}{\partial x_\beta}(a)$ of order $n - k$ are labeled by $\lambda \in \Sigma_{n-k}(m)$ and $\mu \in \Sigma_{n-k}(\beta)$, so that

$$X^{(n-k)} \setminus X^{\text{NMDS}} = X^{(n-k)} \cap \left[\bigcup_{\beta \in \Sigma_{n-k+1}(n)} V \left(\det \frac{\partial f_\lambda}{\partial x_\mu} \mid \lambda \in \Sigma_{n-k}(m), \mu \in \Sigma_{n-k}(\beta) \right) \right].$$

Bearing in mind that $\cup_{\nu \in N} V(S_\nu) = V\left(\prod_{\nu \in N} S_\nu\right)$ for an arbitrary finite set N ,

$$\prod_{\nu \in N} S_\nu := \left\{ \prod_{\nu \in N} g_\nu \mid g_\nu \in S_\nu \right\}$$

and arbitrary subsets $S_\nu \subset \overline{\mathbb{F}_q}[x_1, \dots, x_n]$, one concludes that

$$X^{(n-k)} \setminus X^{\text{NMDS}} = X^{(n-k)} \cap V\left(\prod_{\beta \in \Sigma_{n-k+1}(n)} \det \frac{\partial f_{\psi(\beta)}}{\partial x_{\theta(\beta)}} \mid \begin{array}{l} \psi : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(m), \\ \theta : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(n), \\ \theta(\beta) \in \Sigma_{n-k}(\beta) \end{array}\right)$$

Therefore, the subset X^{NMDS} of $X^{(n-k)}$ equals

$$X^{\text{NMDS}} = X^{(n-k)} \setminus (X^{(n-k)} \setminus X^{\text{NMDS}}) = X^{(n-k)} \setminus V(A)$$

for

$$A := \left\{ \prod_{\beta \in \Sigma_{n-k+1}(n)} \det \frac{\partial f_{\psi(\beta)}}{\partial x_{\theta(\beta)}} \mid \begin{array}{l} \psi : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(m), \\ \theta : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(n), \\ \theta(\beta) \in \Sigma_{n-k}(\beta) \end{array} \right\}.$$

If

$$B := \left\{ \prod_{i \in \Sigma_{n-k-1}(n)} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \mid \varphi : \Sigma_{n-k-1}(n) \rightarrow \Sigma_{n-k-1}(m) \right\}$$

the by Proposition 2 (ii) and (1) there follows

$$X^{(n-k)} = X^{(\geq n-k)} = X \setminus X^{(\leq n-k-1)} = X \setminus V(B).$$

Thus,

$$X^{\text{NMDS}} = [X \setminus V(B)] \setminus V(A) = X \setminus [V(B) \cup V(A)] = X \setminus V(BA)$$

with

$$BA = \left\{ \prod_{i \in \Sigma_{n-k-1}(n)} \det \frac{\partial f_{\varphi(i)}}{\partial x_i} \prod_{\beta \in \Sigma_{n-k+1}(n)} \det \frac{\partial f_{\psi(\beta)}}{\partial x_{\theta(\beta)}} \mid \begin{array}{l} \varphi : \Sigma_{n-k-1}(n) \rightarrow \Sigma_{n-k-1}(m), \\ \psi : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(m), \\ \theta : \Sigma_{n-k+1}(n) \rightarrow \Sigma_{n-k}(n), \\ \theta(\beta) \in \Sigma_{n-k}(\beta) \end{array} \right\}.$$

By Lemma 3.2 from [4], a linear code C is near MDS if and only if its dual C^\perp is near MDS. Thus, at any $a \in X^{\text{NMDS}}$ the gradient code $\text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})$ is near MDS and, in particular, $d(\text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})) = k$. In such a way, $X^{\text{NMDS}} \subseteq X_{\text{grad}}^{(\geq k)}$ and $X_{\text{grad}}^{(\geq k)}$ is Zariski dense in X . By Proposition 11, the presence of a non-zero polynomial $h \in I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\gamma]$ requires the Zariski closure $\overline{X_{\text{grad}}^{(\geq k)}} \subseteq \Pi_{\neg\gamma}^{-1}(\Pi_{\neg\gamma}(X)^{\text{sing}}) \subsetneq X$ to be a proper affine subvariety of X . The contradiction justifies the vanishing of the intersections $I(X, \overline{\mathbb{F}_q}) \cap \overline{\mathbb{F}_q}[x_\gamma] = \{0\}$ for $\forall \gamma \in \Sigma_{k-1}(n)$. \square

By Theorem 3.5 from [4], the existence of an $[n, k, n-k]_q$ -code with $k \geq 2$ requires $n - k \leq 2q$. Therefore $X^{(n-k)} \subseteq \cup_{q^l \geq \frac{n-k}{2}} X(\mathbb{F}_{q^l})$ in the case of $\dim X = k \geq 2$. Theorem 3.4 from [4] specifies that for $q < n - k$ any $[n, k, n-k]_q$ -code is near MDS. Thus, $X^{(n-k)} \setminus X^{\text{NMDS}} \subseteq \cup_{q^l \geq n-k} X^{(n-k)}(\mathbb{F}_{q^l})$. Note that

$$Y = \cup_{q^l < n-k} X^{(n-k)}(\mathbb{F}_{q^l}) = X^{(n-k)} \cap \left[\cup_{q^l < n-k} V(x_i^{q^l} - x_i \mid 1 \leq i \leq n) \right] = X^{(n-k)} \setminus \cup_{q^l \geq n-k} X^{(n-k)}(\mathbb{F}_{q^l})$$

is a finite explicitly given affine subvariety of $X^{(n-k)}$, contained in X^{NMDS} . Therefore $\dim Y = 0$, while $\dim X^{\text{NMDS}} = k$ and X^{NMDS} is "considerably larger" than Y .

5.2 Cyclic tangent codes

Let us recall that a linear code $C \subset \mathbb{F}_q^n$ is cyclic if invariant under the cyclic shift of components

$$\zeta : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n, \\ \zeta(x_1, x_2, \dots, x_n) = (x_2, \dots, x_n, x_1).$$

The cyclic codes C are in a bijective correspondence with the principal ideals $\langle \bar{g} \rangle_{\mathbb{F}_q} \triangleleft \mathbb{F}_q[t] / \langle t^n - 1 \rangle$ in the quotient ring of $\mathbb{F}_q[t]$ by the ideal $\langle t^n - 1 \rangle \triangleleft \mathbb{F}_q[t]$ with generator $t^n - 1 \in \mathbb{F}_q[t]$. The polynomial $g(t) \in \mathbb{F}_q[t]$ is a divisor of $t^n - 1$ of degree $\deg g = n - \dim_{\mathbb{F}_q} C$ with leading coefficient 1.

In order to construct an affine variety, at which all Zariski tangent spaces extend to cyclic codes over sufficiently large extensions of the definition fields, we need the following

Lemma 13. *Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible k -dimensional affine variety, whose absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ is generated by some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$ and*

$$X_{\leq r} := \left\{ a \in X \mid \text{rk} \frac{\partial f}{\partial x}(a) \leq r \right\} \quad \text{for } 0 \leq r \leq n - k$$

be the loci at which the Zariski tangent spaces are of dimension $\geq n - r$. For an arbitrary \mathbb{F}_{q^s} -linear code $C \subset \mathbb{F}_{q^s}^n$ consider the locus

$$X(C) := \{ a \in X \mid T_a(X, \mathbb{F}_{q^{\delta(a)}}) \otimes_{\mathbb{F}_{q^{\delta(a)}}} \mathbb{F}_{q^{l(a)}} = C \otimes_{\mathbb{F}_{q^s}} \otimes_{\mathbb{F}_{q^{l(a)}}} \text{ for } l(a) = \text{LCM}(\delta(a), s) \in \mathbb{N} \}$$

of X at which the tangent codes coincide with C after an appropriate extension of the constant field.

(i) *The loci*

$$X_{\leq r} = V \left(\det \frac{\partial f_\lambda}{\partial x_\mu} \mid \lambda \in \Sigma_{r+1}(1, \dots, m), \mu \in \Sigma_{r+1}(1, \dots, n) \right) \cap X$$

are Zariski closed subsets of X .

In particular, $X_{\leq n-k-1} = X^{\text{sing}}$ is the set of the singular points of X .

(ii) If $C \subset \mathbb{F}_{q^s}^n$ has parity check matrix $H \in M_{r \times n}(\mathbb{F}_{q^s})$ of rank $0 \leq r \leq n - k$ and H_λ is the matrix, formed by the columns of H , labeled by $\lambda \subseteq \{1, \dots, n\}$, then $X(C) = Z(C) \cap X_{>r-1}$ is the intersection of the Zariski closed subset

$$Z(C) := V \left(\det \left(\begin{array}{c} \frac{\partial f_j}{\partial x_\lambda} \\ H_\lambda \end{array} \right) \mid 1 \leq j \leq m, \lambda \in \Sigma_{r+1}(1, \dots, n) \right) \cap X$$

of X with the Zariski open subset $X_{>r-1} := X \setminus X_{\leq r-1}$. In particular, if $\dim Z(C) \geq 1$ then $X(C)$ is an infinite set.

(iii) For an \mathbb{F}_q -linear code $C \subset \mathbb{F}_q^n$ of $\dim_{\mathbb{F}_q} C = k$ with parity check matrix $H \in M_{(n-k) \times n}(\mathbb{F}_q)$ and for arbitrary polynomials $g_1, \dots, g_{n-k} \in \mathbb{F}_q[x_1, \dots, x_n]$, the affine variety $X_C := V(f_1, \dots, f_{n-k})$ cut by

$$f_i(x_1, \dots, x_n) = \sum_{j=1}^n H_{ij}x_j + g_i(x_1^p, \dots, x_n^p) \quad \text{with} \quad \forall 1 \leq i \leq n - k$$

is smooth and has constant tangent codes $T_a(X, \mathbb{F}_{q^{\delta(a)}}) = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^{\delta(a)}}$ for $\forall a \in X$, i.e., $X_C = X(C)$.

Proof. (i) The condition $\text{rk} \frac{\partial f}{\partial x}(a) \leq r$ is equivalent to the vanishing of all the minors of $\frac{\partial f}{\partial x}(a)$ of order $r + 1$.

(ii) Note that $a \in X \setminus X_{\leq r-1}$ exactly when $\text{rk} \frac{\partial f}{\partial x}(a) \geq r$, which is tantamount to

$$\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) \otimes_{\mathbb{F}_{q^{\delta(a)}}} \mathbb{F}_{q^{l(a)}} \leq n - r = \dim_{\mathbb{F}_{q^{l(a)}}} C \otimes_{\mathbb{F}_{q^s}} \mathbb{F}_{q^{l(a)}}$$

for $l(a) = LCM(\delta(a), s) \in \mathbb{N}$. Thus, a point $a \in X \setminus X_{\leq r-1}$ belongs to $X(C)$ if and only if $T_a(X, \mathbb{F}_{q^{\delta(a)}}) \otimes_{\mathbb{F}_{q^{\delta(a)}}} \mathbb{F}_{q^{l(a)}} \supseteq C \otimes_{\mathbb{F}_{q^s}} \mathbb{F}_{q^{l(a)}}$. This is equivalent to the opposite inclusion of the corresponding dual codes,

$$\text{Span}_{\mathbb{F}_{q^{l(a)}}} \left(\frac{\partial f_j}{\partial x}(a) \mid 1 \leq j \leq m \right) \subseteq \text{RowSpan}_{\mathbb{F}_{q^{l(a)}}} H.$$

Note that $\frac{\partial f_j}{\partial x}(a) \in \text{RowSpan}_{\mathbb{F}_{q^{l(a)}}} H$ if and only if

$$\text{rk} \left(\begin{array}{c} \frac{\partial f_j}{\partial x}(a) \\ H \end{array} \right) = \text{rk} H = r$$

and this is equivalent to the vanishing of all the minors of

$$\left(\begin{array}{c} \frac{\partial f_j}{\partial x}(a) \\ H \end{array} \right) \in M_{(r+1) \times n}(\mathbb{F}_{q^{l(a)}})$$

of order $r + 1$.

(iii) Note that the Jacobian matrix $\frac{\partial(f_1, \dots, f_{n-k})}{\partial(x_1, \dots, x_n)} \equiv H$ is constant and

$$T_a(X_C, \mathbb{F}_{q^{\delta(a)}}) \subseteq C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^{\delta(a)}},$$

according to $f_1, \dots, f_{n-k} \in I(X_C, \overline{\mathbb{F}_q})$. Making use of

$$k \leq \dim X_C \leq \dim T_a(X_C, \mathbb{F}_{q^{\delta(a)}}) \leq \dim_{\mathbb{F}_q} C = k,$$

one concludes that $\dim X_C = k$, $T_a(X_C, \mathbb{F}_{q^{\delta(a)}}) = C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^{\delta(a)}}$ and X_C consists of smooth points. \square

With some abuse of notation, if $X = X(C)$ for some linear code $C \subset \mathbb{F}_q^n$, we say that X has constant Zariski tangent bundles over all finite fields $\mathbb{F}_{q^s} \subset \overline{\mathbb{F}_q}$.

Denote $p = \text{char} \mathbb{F}_q$ and note that $t^n - 1 \in \mathbb{F}_p[t]$ has coefficients from the prime field \mathbb{F}_p of \mathbb{F}_q . For any prime integer p and any natural number n , let \mathbb{F}_σ , $\sigma = \sigma(p, n)$ be the splitting field of $t^n - 1 \in \mathbb{F}_p[t]$ over \mathbb{F}_p . We assume that p and n are relatively prime, so that $t^n - 1$ has no multiple roots in the algebraic closure $\overline{\mathbb{F}_p} = \bigcup_{s=1}^{\infty} \mathbb{F}_{p^s}$ of \mathbb{F}_p . For an arbitrary divisor $g(t) \in \mathbb{F}_\sigma[t]$ of $t^n - 1$ with leading coefficient 1 and an arbitrary $s \in \mathbb{N}$, let us denote by

$$\langle \bar{g} \rangle_{\mathbb{F}_{\sigma^s}} := \langle g(t) + \langle t^n - 1 \rangle_{\mathbb{F}_{\sigma^s}} \rangle \triangleleft \mathbb{F}_{\sigma^s}[t] / \langle t^n - 1 \rangle_{\mathbb{F}_{\sigma^s}}$$

the cyclic code over \mathbb{F}_{σ^s} with generator polynomial $g(t)$. We are interested in the cyclic codes $\langle \bar{g} \rangle_{\mathbb{F}_{\sigma^s}} \subset \mathbb{F}_{\sigma^s}^n$ over \mathbb{F}_{σ^s} of length n and dimension

$$k \leq \dim_{\mathbb{F}_{\sigma^s}} \langle \bar{g} \rangle_{\mathbb{F}_{\sigma^s}} = n - \deg g \leq n.$$

These correspond to $g(t) \in \mathbb{F}_\sigma[t]$ of degree $0 \leq \deg g \leq n - k$.

Denote by $\mathcal{D}_{p,n}$ the set of the divisors $g(t) \in \overline{\mathbb{F}_p}[t]$ of $t^n - 1 \in \mathbb{F}_p[t]$ with leading coefficient 1 and put $\mathcal{D}_{p,n}(\nu) := \{g \in \mathcal{D}_{p,n} \mid \deg g = \nu\}$. Note that $\mathcal{D}_{p,n}$ and therefore $\mathcal{D}_{p,n}(\nu)$ are finite sets. We say that all cyclic codes of length n and dimension k over $\overline{\mathbb{F}_p}$ are realized as finite Zariski tangent spaces to an affine variety $X \subset \overline{\mathbb{F}_p}^n$ of $\dim X = k$, if for any $g \in \mathcal{D}_{p,n}(n - k)$ there exists $a \in X$ with

$$T_a(X, \mathbb{F}_{q^{\delta(a)}}) \otimes_{\mathbb{F}_{q^{\delta(a)}}} \mathbb{F}_{q^{\delta(a,g)}} = \langle \bar{g} \rangle_{\mathbb{F}_{q^{\delta(g)}}} \otimes_{\mathbb{F}_{q^{\delta(g)}}} \mathbb{F}_{q^{\delta(a,g)}},$$

where $\mathbb{F}_{q^{\delta(g)}}$ is the common definition field of all the coefficients of $g(t) \in \overline{\mathbb{F}_p}[t]$ and $\mathbb{F}_{q^{\delta(a,g)}}$ is the common definition field of a and the coefficients of $g(t)$. All cyclic codes of length n over $\overline{\mathbb{F}_p}$ are realized as finite Zariski tangent spaces to an affine variety $X \subset \overline{\mathbb{F}_p}^n$ if this holds for all cyclic codes of length n and an arbitrary dimension $0 \leq k \leq n$ over $\overline{\mathbb{F}_p}$.

The next corollary constructs an affine variety, whose all finite Zariski tangent spaces are cyclic codes and an affine variety with an arbitrary number of non-cyclic tangent codes.

Corollary 14. (i) Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible k -dimensional affine variety, defined over \mathbb{F}_q ,

$$XT^\zeta := \{a \in X \mid \zeta T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_a(X, \mathbb{F}_{q^{\delta(a)}})\}$$

be the subset of X , at which the finite Zariski tangent spaces are cyclic codes and $X^{\text{smooth}} = X_{\geq n-k} = X_{n-k} := \{a \in X \mid \text{rk} \frac{\partial f}{\partial x}(a) = n-k\}$ be the smooth locus of X . Then $XT^\zeta \cap X^{\text{smooth}}$ is a Zariski closed subset of X^{smooth} .

(ii) For an arbitrary natural number n and an arbitrary prime integer p , relatively prime to n , there exists a smooth affine variety

$$X_{p,n}^\zeta := \coprod_{g \in \mathcal{D}_{p,n}} X_{\langle \bar{g} \rangle_{\mathbb{F}_q}} \subset \overline{\mathbb{F}_p}^n,$$

such that all cyclic codes of length n over $\overline{\mathbb{F}_p}$ are realized as Zariski tangent spaces to $X_{p,n}^\zeta$ and all finite Zariski tangent spaces to $X_{p,n}^\zeta$ are cyclic codes.

(iii) For arbitrary $k, n, M \in \mathbb{N}$ with $k < n$ and an arbitrary prime integer p with $\text{GCD}(p, n) = 1$, there is an affine variety $X_{p,n,k}(M) \subset \overline{\mathbb{F}_p}^n$ of $\dim X_{p,n,k}(M) = k$, such that all cyclic codes of length n and dimension k over $\overline{\mathbb{F}_p}$ are realized as finite Zariski tangent spaces to $X_{p,n,k}(M)$ and there are at least M non-cyclic finite Zariski tangent spaces to $X_{p,n,k}(M)$.

Proof. (i) For an arbitrary $0 \leq r \leq n-k$ let us consider the subset

$$XT_r^\zeta := \{a \in XT^\zeta \mid \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = n-r\}$$

of XT^ζ . It suffices to show that

$$XT_r^\zeta = Z_r^\zeta \cap X_{\geq r}$$

is the intersection of a Zariski closed subset $Z_r^\zeta \subseteq X$ with the Zariski open subset $X_{>r-1} := X \setminus X_{\leq r-1}$ of X . In the notations of Lemma 13 (ii), one has

$$\begin{aligned} XT_r^\zeta &= \cup_{g \in \mathcal{D}_{p,n}(n-r)} X(\langle \bar{g} \rangle_{\mathbb{F}_q}) = \\ &= \cup_{g \in \mathcal{D}_{p,n}(n-r)} [Z(\langle \bar{g} \rangle_{\mathbb{F}_q}) \cap X_{>r-1}] = \\ &= [\cup_{g \in \mathcal{D}_{p,n}(n-r)} Z(\langle \bar{g} \rangle_{\mathbb{F}_q})] \cap X_{>r-1} = \\ &= Z_r^\zeta \cap X_{\geq r} \end{aligned}$$

for the Zariski closed subset

$$Z_r^\zeta := \cup_{g \in \mathcal{D}_{p,n}(n-r)} Z(\langle \bar{g} \rangle_{\mathbb{F}_q}) \subseteq X.$$

In the case of $r = n-k$, one concludes that

$$XT_{n-k}^\zeta = Z_{n-k}^\zeta \cap X_{\geq n-k} = Z_{n-k}^\zeta \cap X_{n-k} = XT^\zeta \cap X^{\text{smooth}}$$

is a Zariski closed subset of X^{smooth} .

(ii) In the notations from Lemma 13 (iii), $X_{\langle \bar{g} \rangle_{\mathbb{F}_q}}$ are smooth affine varieties whose all finite Zariski tangent spaces

$$T_a(X_{\langle \bar{g} \rangle_{\mathbb{F}_q}}, \mathbb{F}_{q^{\delta(a)}}) = \langle \bar{g} \rangle_{\mathbb{F}_q} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^{\delta(a)}} = \langle \bar{g} \rangle_{\mathbb{F}_q^{\delta(a)}} \subset \mathbb{F}_{q^{\delta(a)}}^n$$

are cyclic codes.

(iii) For an arbitrary natural number n and an arbitrary prime integer p , which is relatively prime to n , there are $|\mathcal{D}_{p,n}(n-k)| = \binom{n}{n-k} = \binom{n}{k}$ generator polynomials $g(t)$ of cyclic codes of dimension k over $\overline{\mathbb{F}_p}$. These $g(t)$ are uniquely determined by their $n-k$ roots, contained in the set of the n distinct roots of $t^n - 1$ in $\overline{\mathbb{F}_p}$. For any $M \in \mathbb{N}$ there exists $s \in \mathbb{N}$, such that $p^s - \binom{n}{k} \geq M$ and \mathbb{F}_{p^s} contains the splitting fields of all $g \in \mathcal{D}_{p,n}(n-k)$. Consider a family $\mathcal{C} \rightarrow \mathbb{F}_{p^s}^n$ of \mathbb{F}_{p^s} -linear codes $\mathcal{C}(a) \subset \mathbb{F}_{p^s}^n$ of length n and dimension k , which contains all cyclic codes $\langle \bar{g} \rangle_{\mathbb{F}_{p^s}}$ with generator polynomials $g \in \mathcal{D}_{p,n}(n-k)$ as fibres over some points of $\mathbb{F}_{p^s}^n$, and has at least M non-cyclic fibres $\mathcal{C}(b)$, $b \in \mathbb{F}_{p^s}^n$. By Proposition 5, there exist irreducible k -dimensional affine varieties $Y_1/\mathbb{F}_{p^s}, \dots, Y_m/\mathbb{F}_{p^s} \subset \overline{\mathbb{F}_p}^n$, defined over \mathbb{F}_{p^s} , such that

$$\mathbb{F}_{p^s} \subseteq Y_1^{\text{smooth}}(\mathbb{F}_{p^s}) \cup \dots \cup Y_m^{\text{smooth}}(\mathbb{F}_{p^s}) \quad \text{and} \\ T_a(Y_i, \mathbb{F}_{p^s}) = \mathcal{C}(a) \quad \text{for all } a \in \mathbb{F}_{p^s} \quad \text{and all } Y_i \ni a.$$

The affine variety $X_{p,n,k}(M) := Y_1 \cup \dots \cup Y_m$ of dimension k realizes all cyclic codes $\langle \bar{g} \rangle_{\mathbb{F}_{p^s}}$ of length n and dimension k as Zariski tangent spaces and has at least M non-cyclic Zariski tangent codes over \mathbb{F}_{p^s} . □

5.3 Hamming tangent codes

Let us fix a finite field \mathbb{F}_q , a natural number $r \in \mathbb{N}$ and denote $n = |\mathbb{P}^{r-1}(\mathbb{F}_q)| = \frac{q^r - 1}{q - 1}$. Choose a complete set of liftings $H_1, \dots, H_n \in M_{r \times n}(\mathbb{F}_q)$ of the points of the projective space $\mathbb{P}^{r-1}(\mathbb{F}_q) = \mathbb{P}(\mathbb{F}_q^r) \simeq \mathbb{F}_q^r \setminus \{0^r\}/\mathbb{F}_q^*$ or a complete set of \mathbb{F}_q^* -orbit representatives on \mathbb{F}_q^r . The \mathbb{F}_q -linear code $\mathcal{H}_{q,r} \subset \mathbb{F}_q^n$ with parity check matrix $H_{q,r} := (H_1 \dots H_n)$ has minimum distance 3 and is known as the Hamming code. The present subsection constructs an embedding of $\overline{\mathbb{F}_q}^{n-r}$ in $\overline{\mathbb{F}_q}^n$, whose image has $q(q-1)^{n-r-1}$ Hamming tangent codes in the case of an odd characteristic $\text{char}\mathbb{F}_q$ and q^{n-r} Hamming tangent codes for $\text{char}\mathbb{F}_q = 2$.

Proposition 15. *Let $H_{q,r} = (H_1 \dots H_n) \in M_{r \times n}(\mathbb{F}_q)$ with $n = \frac{q^r - 1}{q - 1}$ be a parity check matrix of a Hamming code with $\text{rk}(H_1 \dots H_r) = r$ and $H_{r-1} + H_r = H_{r+1}$. Then the puncturing $\Pi_\rho : \overline{\mathbb{F}_q}^n \rightarrow \overline{\mathbb{F}_q}^{n-r}$ at $\rho = \{1, \dots, r\}$ restricts to a biregular morphism $\Pi_\rho : X = V(f_1, \dots, f_r) \rightarrow \overline{\mathbb{F}_q}^{n-r}$ of the affine variety X , cut by the polynomials*

$$f_i(x_1, \dots, x_n) = \sum_{j=1}^n H_{ij}x_j + \sum_{j=r+2}^n H_{ij}x_j^2 \quad \text{for } 1 \leq i \leq r.$$

If $p = \text{char}\mathbb{F}_q \geq 3$ then $T_a(X, \mathbb{F}_q) \subset \mathbb{F}_q^n$ are Hamming codes for all

$$a \in X(\mathbb{F}_q) \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right)$$

and

$$\left| X(\mathbb{F}_q) \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right) \right| = q(q-1)^{n-r-1}.$$

In the case of $\text{char}\mathbb{F}_q = 2$, the Zariski tangent spaces $T_a(X, \mathbb{F}_q) \subset \mathbb{F}_q^n$ are Hamming codes for all the \mathbb{F}_q -rational points $a \in X(\mathbb{F}_q)$ and $|X(\mathbb{F}_q)| = q^{n-r}$.

Proof. Let us denote

$$A := (H_1 \dots H_r)^{-1} \in M_{r \times r}(\mathbb{F}_q), \quad H'' := (H_{r+2} \dots H_n) \in M_{r \times (n-r-1)}(\mathbb{F}_q)$$

and observe that

$$\begin{pmatrix} f_1 \\ \dots \\ f_r \end{pmatrix} = \begin{pmatrix} A^{-1} & H_{r+1} & H'' \end{pmatrix} \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} + H'' \begin{pmatrix} x_{r+2}^2 \\ \dots \\ x_n^2 \end{pmatrix}.$$

Therefore

$$A \begin{pmatrix} f_1 \\ \dots \\ f_r \end{pmatrix} = \begin{pmatrix} I_r & (AH_{r+1}) & (AH'') \end{pmatrix} \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} + (AH'') \begin{pmatrix} x_{r+2}^2 \\ \dots \\ x_n^2 \end{pmatrix}$$

and

$$A \begin{pmatrix} f_1 \\ \dots \\ f_r \end{pmatrix} = x_i + (AH_{r+1})_i x_{r+1} + \sum_{j=r+2}^n (AH'')_{ij} x_j (x_j + 1) \quad \text{for } \forall 1 \leq i \leq r. \quad (4)$$

Denote

$$g_i(x_{r+1}, \dots, x_n) := -(AH_{r+1})_i x_{r+1} - \sum_{j=r+2}^n (AH'')_{ij} x_j (x_j + 1) \in \mathbb{F}_q[x_{r+1}, \dots, x_n]$$

for $\forall r+1 \leq i \leq n$. The fiber of the puncturing $\Pi_\rho : X \rightarrow \overline{\mathbb{F}}_q^{n-r}$ over an arbitrary point $a' = (a_{r+1}, \dots, a_n) \in \overline{\mathbb{F}}_q^{n-r}$ is claimed to consist of a single point

$$\Pi_\rho^{-1}(a') \cap X = \{(g_1(a'), \dots, g_r(a'), a')\}. \quad (5)$$

Indeed, if $a = (a_1, \dots, a_r, a') \in \Pi_\rho^{-1}(a') \cap X$ then $f_1(a) = \dots = f_r(a) = 0$ and (4) implies that $a_i - g_i(a') = 0$ for $\forall 1 \leq i \leq r$. Conversely, if $a_i = g_i(a')$ for $\forall 1 \leq i \leq r$ then (4) requires

$$A \begin{pmatrix} f_1(a) \\ \dots \\ f_r(a) \end{pmatrix} = 0_{r \times 1},$$

whereas

$$\begin{pmatrix} f_1(a) \\ \dots \\ f_r(a) \end{pmatrix} = A^{-1} 0_{r \times 1} = (H_1 \dots H_r) 0_{r \times 1} = 0_{r \times 1}$$

and $(g_1(a'), \dots, g_r(a'), a') \in \Pi_\rho^{-1}(a') \cap X$. In such a way,

$$\Pi_\rho^{-1} : \overline{\mathbb{F}}_q^{n-r} \longrightarrow X,$$

$$\Pi_\rho^{-1}(x_{r+1}, \dots, x_n) = (g_1(x_{r+1}, \dots, x_n), \dots, g_r(x_{r+1}, \dots, x_n), x_{r+1}, \dots, x_n)$$

is a correctly defined morphism of affine varieties and $\Pi_\rho : X \rightarrow \overline{\mathbb{F}_q}^{n-r}$ is a biregular map.

According to

$$\frac{\partial f_i}{\partial x_j} = H_{ij} \quad \text{for } 1 \leq j \leq r+1, \quad 1 \leq i \leq r \quad \text{and}$$

$$\frac{\partial f_i}{\partial x_j} = H_{ij}(1 + 2x_j) \quad \text{for } r+2 \leq j \leq n, \quad 1 \leq i \leq r,$$

the Jacobian matrix of the defining equations of X is

$$\frac{\partial f}{\partial x} = (H_1 \dots H_r [(1 + 2x_{r+2})H_{r+2}] \dots [(1 + 2x_n)H_n]).$$

Due to $H_{r-1} + H_r - H_{r+1} = 0_{r \times 1}$, the word $c := (0^{r-2}, 1, 1, -1, 0^{n-r-1})$ belongs to all tangent codes $T_b(X, \mathbb{F}_q^{\delta(b)})$, $b \in X$. Therefore $d(T_b(X, \mathbb{F}_q^{\delta(b)})) \leq 3$ and $X = X^{(\leq 3)}$.

If $\text{char} \mathbb{F}_q = 2$ then $\frac{\partial f}{\partial x}(a) = H_{q,r}$ for all $a \in X$ and $T_a(X, \mathbb{F}_q)$ are Hamming codes at all the \mathbb{F}_q -rational points $a \in X(\mathbb{F}_q)$. Note that the polynomials

$$g_1(x_{r+1}, \dots, x_n), \dots, g_r(x_{r+1}, \dots, x_n)$$

have coefficients from \mathbb{F}_q , so that for any $a' \in \mathbb{F}_q^{n-r}$ one has $\Pi_\rho^{-1}(a') \cap X \subseteq X(\mathbb{F}_q)$. Thus, $\Pi_\rho : X \rightarrow \overline{\mathbb{F}_q}^{n-r}$ restricts to a bijective map $\Pi_\rho : X(\mathbb{F}_q) \rightarrow \mathbb{F}_q^{n-r}$ and the cardinality $|X(\mathbb{F}_q)| = |\mathbb{F}_q^{n-r}| = q^{n-r}$.

If $\text{char} \mathbb{F}_q = p \geq 3$ is an odd prime then for any $a \in X(\mathbb{F}_q) \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right)$ the columns of $\frac{\partial f}{\partial x}(a)$ are pairwise non-proportional. Therefore $\frac{\partial f}{\partial x}(a)$ is a parity check matrix of the Hamming code $\mathcal{H}_{q,r} = T_a(X, \mathbb{F}_q)$ for $\forall a \in X(\mathbb{F}_q) \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right)$. The bijective map $\Pi_\rho : X(\mathbb{F}_q) \rightarrow \mathbb{F}_q^{n-r}$ restricts to an isomorphism

$$\Pi_\rho : X(\mathbb{F}_q) \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right) \longrightarrow \mathbb{F}_q^{n-r} \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right).$$

Making use of

$$\mathbb{F}_q^{n-r} \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right) \simeq \mathbb{F}_q \times (\mathbb{F}_q \setminus \{-[2(\text{mod } p)]^{-1}\})^{n-r-1},$$

one concludes that $\left| X(\mathbb{F}_q) \setminus V \left(\prod_{j=r+2}^n (2x_j + 1) \right) \right| = q(q-1)^{n-r-1}$.

□

6 Operations on tangent codes and affine varieties

6.1 Tangent codes to punctured varieties

The present section provides a sufficient condition for a Zariski tangent space to the punctured variety $\Pi_\gamma(X)$ to be the puncturing at γ of the corresponding Zariski tangent space to X . This is shown to hold on a Zariski dense subset W_t of X . The tangent vectors to $\Pi_\gamma(X)$ of minimum weight at the points of $\Pi_\gamma(W_\gamma)$ turn to be the puncturings at γ of the tangent vectors to X of minimum weight, containing γ in its support.

Lemma 16. *For any puncturing $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ of a k -dimensional affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^N$ with l -dimensional generic fibres $\Pi_\gamma^{-1}(\Pi_\gamma(a))$, $a \in X$, there exists a factorization*

$$\begin{array}{ccc} X & \xrightarrow{\Pi_{\gamma \setminus \beta}} & \Pi_{\gamma \setminus \beta}(X) \\ \Pi_\gamma \downarrow & \searrow \Pi_\beta & \\ \Pi_\gamma(X) & & \end{array}$$

through a finite puncturing $\Pi_{\gamma \setminus \beta} : X \rightarrow \Pi_{\gamma \setminus \beta}(X)$, followed by a puncturing $\Pi_\beta : \Pi_{\gamma \setminus \beta}(X) \rightarrow \Pi_\gamma(X)$ with generic fibres $\overline{\mathbb{F}_q}^l$. Moreover, if the finite puncturing $\Pi_{\gamma \setminus \beta} : X \rightarrow \Pi_{\gamma \setminus \beta}(X)$ is separable then there is a Zariski dense subset

$$U_{\gamma \setminus \beta} := \text{Etale}(\Pi_{\gamma \setminus \beta}) \cap \Pi_{\gamma \setminus \beta}^{-1}(\Pi_{\gamma \setminus \beta}(X)^{\text{smooth}}) \subseteq X,$$

at which the puncturings

$$\Pi_\gamma T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_{\Pi_\gamma(a)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) \quad (6)$$

of the tangent codes to X at γ are tangent codes to the puncturing $\Pi_\gamma(X)$ of X at γ .

Proof. The surjective morphism $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ induces an embedding $\Pi_\gamma^* : \overline{\mathbb{F}_q}(\Pi_\gamma(X)) \hookrightarrow \overline{\mathbb{F}_q}(X)$ of the corresponding function fields. The transcendence degree $\text{trdeg}_{\overline{\mathbb{F}_q}(\Pi_\gamma(X))} \overline{\mathbb{F}_q}(X)$ of $\overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ coincides with the dimension l of a generic fibre of $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$. If $\overline{x_\beta} = \{\overline{x_{\beta_1}}, \dots, \overline{x_{\beta_l}}\}$, $\overline{x_{\beta_i}} := x_{\beta_i} + I(X, \overline{\mathbb{F}_q}) \in \overline{\mathbb{F}_q}[X] \subset \overline{\mathbb{F}_q}(X)$ is a coordinate transcendence basis of $\overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ for a subset $\beta \subseteq \gamma$ then the field $\overline{\mathbb{F}_q}(\Pi_\gamma(X))(\overline{x_\beta}) = \overline{\mathbb{F}_q}(\Pi_{\gamma \setminus \beta}(X))$ is a purely transcendental extension of $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ of degree l and $\overline{\mathbb{F}_q}(X)$ is a finite extension of $\overline{\mathbb{F}_q}(\Pi_{\gamma \setminus \beta}(X))$. Thus, $\Pi_{\gamma \setminus \beta} : X \rightarrow \Pi_{\gamma \setminus \beta}(X)$ is a finite morphism and the generic fibres of $\Pi_\beta : \Pi_{\gamma \setminus \beta}(X) \rightarrow \Pi_\gamma(X)$ are isomorphic to the affine space $\overline{\mathbb{F}_q}^l$.

At an arbitrary point $a \in \text{Etale}(\Pi_{\gamma \setminus \beta})$, one has a commutative diagram

$$\begin{array}{ccc} T_a(X, \mathbb{F}_{q^{\delta(a)}}) & \xrightarrow{(d\Pi_{\gamma \setminus \beta})_a} & T_{\Pi_{\gamma \setminus \beta}(a)}(\Pi_{\gamma \setminus \beta}(X), \mathbb{F}_{q^{\delta(a)}}) \\ & \searrow (d\Pi_{\gamma})_a & \downarrow (d\Pi_{\beta})_{\Pi_{\gamma \setminus \beta}(a)} \\ & & T_{\Pi_{\gamma}(a)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(a)}}) \end{array}$$

of puncturings of tangent codes. By the very definition of the étalé locus $\text{Etale}(\Pi_{\gamma \setminus \beta})$ of $\Pi_{\gamma \setminus \beta}$, the $\mathbb{F}_{q^{\delta(a)}}$ -linear map $(d\Pi_{\gamma \setminus \beta})_a$ is injective. Therefore

$$\begin{aligned} & \dim_{\mathbb{F}_{q^{\delta(a)}}} \ker(d\Pi_{\gamma})_a = \\ & \dim_{\mathbb{F}_{q^{\delta(a)}}} \ker(d\Pi_{\beta})_{\Pi_{\gamma \setminus \beta}(a)} : [d(\Pi_{\gamma \setminus \beta})_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow \Pi_{\gamma} T_a(X, \mathbb{F}_{q^{\delta(a)}})] \leq \\ & \dim_{\mathbb{F}_{q^{\delta(a)}}} \ker(d\Pi_{\beta})_{\Pi_{\gamma \setminus \beta}(a)} : [T_{\Pi_{\gamma \setminus \beta}(a)}(\Pi_{\gamma \setminus \beta}(X), \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\Pi_{\gamma}(a)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(a)}})]. \end{aligned}$$

The puncturing $(d\Pi_{\beta})_{\Pi_{\gamma \setminus \beta}(a)} = \Pi_{\beta}$ at $|\beta| = l$ coordinates has kernel of dimension $\leq l$, so that $\dim_{\mathbb{F}_{q^{\delta(a)}}} \ker(d\Pi_{\gamma})_a \leq l$. If $a \in \text{Etale}(\Pi_{\gamma \setminus \beta}) \cap \Pi_{\gamma}^{-1}(\Pi_{\gamma}(X)^{\text{smooth}})$ then $\dim T_{\Pi_{\gamma}(a)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_{\gamma}(X) = k - l$ and the code $(d\Pi_{\gamma})_a T_a(X, \mathbb{F}_{q^{\delta(a)}})$, contained in $T_{\Pi_{\gamma}(a)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(a)}})$ is of dimension

$$k - l \geq \dim_{\mathbb{F}_{q^{\delta(a)}}} (d\Pi_{\gamma})_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) - \dim_{\mathbb{F}_{q^{\delta(a)}}} \ker(d\Pi_{\gamma})_a \geq k - l.$$

As a result,

$$\dim_{\mathbb{F}_{q^{\delta(a)}}} (d\Pi_{\gamma})_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) = k - l = \dim T_{\Pi_{\gamma}(a)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(a)}})$$

and there follows (6). □

Let $C \subset \mathbb{F}_q^n$ be a linear code of minimum distance $d(C) = d$. For any $\nu \in \mathbb{N}$, $\nu \geq d$ denote by

$$\text{Wt}_{\nu}(C) := \{c \in C \mid \text{wt}(c) = \nu\}$$

the set of the words of C of weight ν . The following simple lemma will be used for the description of the words of minimum weight in a generic tangent code to $\Pi_{\gamma}(X)$.

Lemma 17. *Let $C \subset \mathbb{F}_q^n$ be an \mathbb{F}_q -linear code of minimum distance $d(C) = d > s$ and $\Pi_{\gamma} : C \rightarrow \Pi_{\gamma}(C)$ be the puncturing at some $\gamma = \{\gamma_1, \dots, \gamma_s\} \in \Sigma_s(1, \dots, n)$. Then the punctured code $\Pi_{\gamma}(C) \subset \mathbb{F}_q^{n-s}$ is of minimum distance $d(\Pi_{\gamma}(C)) \geq d - s$ and the words*

$$\text{Wt}_{d-s}(\Pi_{\gamma}(C)) = \Pi_{\gamma}(\text{Wt}_d(C) \setminus V(x_{\gamma_1} \dots x_{\gamma_s}))$$

of $\Pi_{\gamma}(C)$ of weight $d - s$ are exactly the punctures of the words $c \in C$ of minimum weight d , whose support contains γ .

In particular, $d(\Pi_{\gamma}(C)) = d - s$ exactly when C contains a word c with support $\text{Supp}(c) \supseteq \gamma$, $|\text{Supp}(c)| = d$.

Proof. By an induction on s , if $\gamma = \{\gamma_1\}$ and $d > 1$ then

$$\text{Wt}_{d-1}(\Pi_{\gamma_1}(C)) = \Pi_{\gamma_1}(\text{Wt}_d(C) \setminus V(\gamma_1)) \quad (7)$$

and $d(\Pi_{\gamma_1}(C)) \geq d - 1$. For an arbitrary $\gamma = \{\gamma_1, \dots, \gamma_{s-1}, \gamma_s\} \in \Sigma_s(1, \dots, n)$, let us denote $\gamma' := \{\gamma_1, \dots, \gamma_{s-1}\} \in \Sigma_{s-1}(1, \dots, n)$ and assume that

$$\text{Wt}_{d-s+1}(\Pi_{\gamma'}(C)) = \Pi_{\gamma'}(\text{Wt}_d(C) \setminus V(x_{\gamma_1} \dots x_{\gamma_{s-1}})), \quad (8)$$

$d(\Pi_{\gamma'}(C)) \geq d - s + 1 > 1$. The application of (7) to $\Pi_{\gamma'}(C)$ provides

$$\text{Wt}_{d-s}(\Pi_{\gamma}(C)) = \text{Wt}_{d-s}(\Pi_{\gamma_s} \Pi_{\gamma'}(C)) = \Pi_{\gamma_s}(\text{Wt}_{d-s+1}(\Pi_{\gamma'}(C)) \setminus V(x_{\gamma_s}))$$

and $d(\Pi_{\gamma}(C)) \geq d - s$. By the inductual hypothesis (8) one has

$$\begin{aligned} \text{Wt}_{d-s+1}(\Pi_{\gamma'}(C)) \setminus V(x_{\gamma_s}) &= \Pi_{\gamma'}(\text{Wt}_d(C) \setminus V(x_{\gamma_1} \dots x_{\gamma_{s-1}})) \setminus V(x_{\gamma_s}) = \\ &= \Pi_{\gamma'}(\text{Wt}_d(C) \setminus V(x_{\gamma_1} \dots x_{\gamma_s})). \end{aligned}$$

Therefore

$$\text{Wt}_{d-s}(\Pi_{\gamma}(C)) = \Pi_{\gamma_s} \Pi_{\gamma'}(\text{Wt}_d(C) \setminus V(x_{\gamma_1} \dots x_{\gamma_s})) = \Pi_{\gamma}(\text{Wt}_d(C) \setminus V(x_{\gamma_1} \dots x_{\gamma_s})).$$

□

Corollary 18. *Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over \mathbb{F}_q with $X^{(d)} := \{a \in X \mid d(T_a(X, \mathbb{F}_q)) = d\} \neq \emptyset$, $\Pi_{\beta} : X \rightarrow \Pi_{\beta}(X)$ be a non-finite puncturing at $|\beta| = d$ variables and $\Pi_{\gamma} : X \rightarrow \Pi_{\gamma}(X)$ be a finite separable puncturing at a subset $\gamma \subset \beta$ of cardinality $|\gamma| = s$. Then*

- (i) *$\text{Etale}(\Pi_{\gamma}) \cap \Pi_{\gamma}^{-1}(\Pi_{\gamma}(X)^{\text{smooth}}) \cap X^{(d)}$ is a Zariski dense subset of X ;*
- (ii) *at any point $b \in \text{Etale}(\Pi_{\gamma}) \cap \Pi_{\gamma}^{-1}(\Pi_{\gamma}(X)^{\text{smooth}}) \cap X^{(d)}$ the tangent code $T_{\Pi_{\gamma}(b)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(b)}}) = (d\Pi_{\gamma})_b T_b(X, \mathbb{F}_{q^{\delta(b)}})$ is of minimum distance $\geq d - s$ and the words*

$$\text{Wt}_{d-s}(T_{\Pi_{\gamma}(b)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(b)}})) = \Pi_{\gamma}(\text{Wt}_d(T_b(X, \mathbb{F}_{q^{\delta(b)}}) \setminus V(x_{\gamma_1} \dots x_{\gamma_s}))$$

of $T_{\Pi_{\gamma}(b)}(\Pi_{\gamma}(X), \mathbb{F}_{q^{\delta(b)}})$ of minimum weight $d - s$ are the punctures of the words of $T_b(X, \mathbb{F}_{q^{\delta(b)}})$ of weight d , whose support contains γ .

Proof. (i) By Proposition 2 (ii), the set $X^{(d)}$ is Zariski dense in X . Then Lemma 1 (iii) applies to Π_{γ} and provides the Zariski density of $U_{\gamma} := \text{Etale}(\Pi_{\gamma}) \cap \Pi_{\gamma}^{-1}(\Pi_{\gamma}(X)^{\text{smooth}})$ in X . The inclusions

$$U_{\gamma} \cap X^{(d)} \subseteq U_{\gamma}, \quad U_{\gamma} \cap X^{(d)} \subseteq X^{(d)}$$

of subsets of $\overline{\mathbb{F}_q}^n$ imply the opposite inclusions

$$I(U_{\gamma}, \overline{\mathbb{F}_q}) \subseteq I(U_{\gamma} \cap X^{(d)}, \overline{\mathbb{F}_q}), \quad I(X^{(d)}, \overline{\mathbb{F}_q}) \subseteq I(U_{\gamma} \cap X^{(d)}, \overline{\mathbb{F}_q})$$

of the corresponding absolute ideals. Therefore

$$I(U_{\gamma}, \overline{\mathbb{F}_q}) + I(X^{(d)}, \overline{\mathbb{F}_q}) \subseteq I(U_{\gamma} \cap X^{(d)}, \overline{\mathbb{F}_q}),$$

whereas the Zariski closure

$$\begin{aligned}\overline{U_\gamma \cap X^{(d)}} &= VI(U_\gamma \cap X^{(d)}, \overline{\mathbb{F}_q}) \subseteq V(I(U_\gamma, \overline{\mathbb{F}_q}) + I(X^{(d)}, \overline{\mathbb{F}_q})) = \\ &VI(U_\gamma, \overline{\mathbb{F}_q}) \cap VI(X^{(d)}, \overline{\mathbb{F}_q}) = \overline{U_\gamma} \cap \overline{X^{(d)}} = X \cap X = X.\end{aligned}$$

(ii) The claim is an immediate consequence of Lemma 17 and the surjectiveness of the differential $(d\Pi_\gamma)_b : T_b(X, \mathbb{F}_{q^{\delta(b)}}) \rightarrow T_{\Pi_\gamma(b)}(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(b)}})$ of $\Pi_\gamma : X \rightarrow \Pi_\gamma(X)$ at any point $b \in U_\gamma$, established in Lemma 1 (ii). \square

6.2 Shortening and puncturing tangent and gradient codes

The present subsection describes the shortening of a tangent code to X on γ as a tangent code to the shortening $\Pi_\gamma(X \cap V(x_i | i \in \gamma))$ of the variety X on γ , the puncturing of a gradient code to X at γ as a gradient code to $X \cap V(x_i | i \in \gamma)$ and the shortening of a gradient code to X on γ as a gradient code to the puncturing $\Pi_\gamma(X)$ of X at γ .

The shortening of a linear code $C \subset \mathbb{F}_q^n$ on $\gamma \in \Sigma_s(1, \dots, n)$ is the puncturing

$$C_\gamma := \Pi_\gamma(C \cap V(x_i | \forall i \in \gamma))$$

of the subspace $C \cap V(x_i | \forall i \in \gamma) = \{c \in C \mid c_i = 0, \forall i \in \gamma\}$ of C at γ .

Let $X \subset \overline{\mathbb{F}_q}^n$ be a k -dimensional irreducible affine variety with absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ for some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$. A point $a \in X$ is smooth exactly when $\text{rk} \frac{\partial f}{\partial x}(a) = n - k$. If so, then there exist $\lambda \in \Sigma_{n-k}(1, \dots, m)$ and $\mu \in \Sigma_{n-k}(1, \dots, n)$ with $\det \frac{\partial f_\lambda}{\partial x_\mu}(a) \neq 0$. Denoting

$$X^{\text{smooth}}(\mu) := X \setminus V\left(\det \frac{\partial f_\lambda}{\partial x_\mu} \mid \lambda \in \Sigma_{n-k}(1, \dots, m)\right),$$

one expresses

$$X^{\text{smooth}} = \cup_{\mu \in \Sigma_{n-k}(1, \dots, n)} X^{\text{smooth}}(\mu).$$

Observe that $X^{\text{smooth}}(\mu)$ are Zariski open subsets of X . As far as X^{smooth} is non-empty, Zariski open and Zariski dense in X , there exists $\mu \in \Sigma_{n-k}(1, \dots, n)$ with non-empty and Zariski dense $X^{\text{smooth}}(\mu) \subseteq X$.

Proposition 19. (i) Let $X \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety with absolute ideal $I(X, \overline{\mathbb{F}_q}) = \langle f_1, \dots, f_m \rangle_{\overline{\mathbb{F}_q}}$ for some $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n]$, $X^{\text{smooth}}(\mu) \neq \emptyset$ for some $\mu \in \Sigma_{n-k}(1, \dots, n)$ and $\gamma \in \Sigma_s(\neg\mu)$. Then at an arbitrary point $a \in X^{\text{smooth}}(\mu) \cap \text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}((\Pi_\gamma(X \cap V(x_i | i \in \gamma)))^{\text{smooth}})$ the shortening

$$\begin{aligned}T_a(X, \mathbb{F}_{q^{\delta(a)}})_\gamma &:= \\ \Pi_\gamma(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)) &= T_{\Pi_\gamma(a)}(\Pi_\gamma(X \cap V(x_i | i \in \gamma)), \mathbb{F}_{q^{\delta(a)}})\end{aligned}\tag{9}$$

of a Zariski tangent space to X on γ coincides with the Zariski tangent space to the shortening $X \cap V(x_i | i \in \gamma)$ of X on γ and the puncturing

$$\Pi_\gamma \text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}}) = \text{grad}_{\Pi_\gamma(a)} I(X \cap V(x_i | i \in \gamma), \mathbb{F}_{q^{\delta(a)}})\tag{10}$$

of the gradient code to X at γ coincides with the gradient code to the shortening $X \cap V(x_i | i \in \gamma)$ of X on γ .

(ii) Suppose that $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ is an irreducible affine variety, defined over \mathbb{F}_q , $\gamma \in \Sigma_s(1, \dots, n)$, $\beta \subseteq \gamma$ and x_β is such a coordinate transcendence basis of $\overline{\mathbb{F}_q}(X)$ over $\overline{\mathbb{F}_q}(\Pi_\gamma(X))$ that the finite puncturing $\Pi_{\gamma \setminus \beta} : X \rightarrow \Pi_{\gamma \setminus \beta}(X)$ is separable. Then at any point $a \in \text{Etale}(\Pi_{\gamma \setminus \beta}) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X)^{\text{smooth}})$ the shortening

$$\begin{aligned} \text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}})_\gamma &:= \\ \Pi_\gamma(\text{grad}_a I(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)) &= \text{grad}_{\Pi_\gamma(a)} I(\Pi_\gamma(X), \mathbb{F}_{q^{\delta(a)}}) \end{aligned} \quad (11)$$

of the gradient code to X on γ coincides with the gradient code to the puncturing $\Pi_\gamma(X)$ of X at γ .

Proof. (i) The inclusions $X \cap V(x_i | i \in \gamma) \subseteq X$, $X \cap V(x_i | i \in \gamma) \subseteq V(x_i | i \in \gamma)$ of affine varieties imply the opposite inclusions $I(X, \overline{\mathbb{F}_q}) \subseteq I(X \cap V(x_i | i \in \gamma), \overline{\mathbb{F}_q})$, $\langle x_i | i \in \gamma \rangle_{\overline{\mathbb{F}_q}} \subseteq I(X \cap V(x_i | i \in \gamma), \overline{\mathbb{F}_q})$ of the corresponding absolute ideals. Thus, at any point $a \in X \cap V(x_i | i \in \gamma)$ one has

$$T_a(X \cap V(x_i | i \in \gamma), \mathbb{F}_{q^{\delta(a)}}) \subseteq T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma),$$

whereas

$$\Pi_\gamma T_a(X \cap V(x_i | i \in \gamma), \mathbb{F}_{q^{\delta(a)}}) \subseteq \Pi_\gamma(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)).$$

Moreover, if $a \in \text{Etale}(\Pi_\gamma) \cap \Pi_\gamma^{-1}(\Pi_\gamma(X \cap V(x_i | i \in \gamma))^{\text{smooth}})$ then

$$\Pi_\gamma T_a(X \cap V(x_i | i \in \gamma), \mathbb{F}_{q^{\delta(a)}}) = T_{\Pi_\gamma(a)}(\Pi_\gamma(X \cap V(x_i | i \in \gamma)), \mathbb{F}_{q^{\delta(a)}})$$

and the Zariski tangent space

$$T_{\Pi_\gamma(a)}(\Pi_\gamma(X \cap V(x_i | i \in \gamma)), \mathbb{F}_{q^{\delta(a)}}) \subseteq \Pi_\gamma(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma))$$

to the shortening $\Pi_\gamma(X \cap V(x_i | i \in \gamma))$ of X on γ is contained in the shortening of the Zariski tangent space to X at a . If $a \in X(\mu)^{\text{smooth}}$ then the parity check matrix

$$\begin{pmatrix} \frac{\partial f}{\partial x_\gamma}(a) & \frac{\partial f}{\partial x_{\neg\gamma}}(a) \\ I_\gamma & 0 \end{pmatrix}$$

of $T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)$ is of maximal rank $n - k + s$, due to $\mu \subseteq \neg\gamma$. The non-existence of a non-zero word $c \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)$ with support $\text{Supp}(c) \subseteq \gamma$ reveals the injectiveness of the puncturing

$$(d\Pi_\gamma)_a = \Pi_\gamma : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma) \longrightarrow \mathbb{F}_{q^{\delta(a)}}^{n-|\gamma|}.$$

Therefore

$$\begin{aligned} \dim_{\mathbb{F}_{q^{\delta(a)}}} \Pi_\gamma(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)) &= \\ \dim_{\mathbb{F}_{q^{\delta(a)}}} T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma) &= k - s. \end{aligned}$$

On the other hand, at any smooth point $\Pi_\gamma(a) \in \Pi_\gamma(X \cap V(x_i | i \in \gamma))^{\text{smooth}}$ one has

$$\dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X \cap V(x_i | i \in \gamma)), \mathbb{F}_{q^{\delta(a)}}) = \dim \Pi_\gamma(X \cap V(x_i | i \in \gamma)).$$

Since $\Pi_\gamma : X \cap V(x_i | i \in \gamma) \rightarrow \Pi_\gamma(X \cap V(x_i | i \in \gamma))$ is biregular, there holds $\dim \Pi_\gamma(X \cap V(x_i | i \in \gamma)) = \dim X \cap V(x_i | i \in \gamma) \geq k - s$, whereas

$$\dim T_{\Pi_\gamma(a)}(\Pi_\gamma(X \cap V(x_i | i \in \gamma)), \mathbb{F}_{q^{\delta(a)}}) = \dim_{\mathbb{F}_{q^{\delta(a)}}} \Pi_\gamma(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \cap V(x_i | i \in \gamma)).$$

That justifies (9).

For an arbitrary linear code $C \subset \mathbb{F}_{q^{\delta(a)}}^n$ with dual code $C^\perp \subset \mathbb{F}_{q^{\delta(a)}}^n$ and an arbitrary index set $\gamma \in \Sigma_s(1, \dots, n)$ one has $\Pi_\gamma(C^\perp) = \Pi_\gamma(C \cap V(x_i | i \in \gamma))^\perp$ (cf.[8]). The application of this equality to $C = T_a(X, \mathbb{F}_{q^{\delta(a)}})$ and (9) yields (10).

(ii) Note that $\Pi_\gamma(C^\perp \cap V(x_i | i \in \gamma)) = \Pi_\gamma(C)^\perp$ for an arbitrary linear code $C \subset \mathbb{F}_{q^{\delta(a)}}^n$ with dual code $C^\perp \subset \mathbb{F}_{q^{\delta(a)}}^n$ and an arbitrary $\gamma \in \Sigma_s(1, \dots, n)$ (cf.[8]). Plugging in $C = T_a(X, \mathbb{F}_{q^{\delta(a)}})$ and combining with (6), one obtains (11). \square

6.3 Extension, direct sum and the $(u|u+v)$ construction

For an arbitrary field $\mathbb{F}_q \subseteq F \subseteq \overline{\mathbb{F}_q}$ let

$$\begin{aligned} \varphi_{n+1} : F^n &\longrightarrow F^{n+1}, \\ \varphi_{n+1}(x_1, \dots, x_n) &= \left(x_1, \dots, x_n, -\sum_{i=1}^n x_i \right) \quad \text{for } \forall (x_1, \dots, x_n) \in F^n \end{aligned}$$

be the embedding of F^n in F^{n+1} as the hyperplane with equation

$$x_1 + \dots + x_n + x_{n+1} = 0.$$

The image $\varphi_{n+1}(C) \subset \mathbb{F}_{q^m}^{n+1}$ of a linear code $C \subset \mathbb{F}_{q^m}^n$ is called the extension of C . If $X \subset \overline{\mathbb{F}_q}^n$, is an affine variety then

$$\begin{aligned} \varphi_{n+1} : X &\longrightarrow \varphi_{n+1}(X), \\ \varphi_{n+1} \left(x_1, \dots, x_n \right) &:= \left(x_1, \dots, x_n, -\sum_{i=1}^n x_i \right) \end{aligned}$$

is a biregular morphism and we say that $\varphi_{n+1}(X) \subset \overline{\mathbb{F}_q}^{n+1}$ is the extension of X .

For arbitrary linear codes $C_1 \subset \mathbb{F}_q^n$ and $C_2 \subset \mathbb{F}_q^m$ the direct sum

$$C_1 \oplus C_2 := \{(v_1, v_2) \mid v_1 \in C_1, v_2 \in C_2\} \subset \mathbb{F}_q^{n+m}$$

is a linear code of length $n + m$ and dimension

$$\dim_{\mathbb{F}_q}(C_1 \oplus C_2) = \dim_{\mathbb{F}_q}(C_1) + \dim_{\mathbb{F}_q}(C_2).$$

It is easy to observe that the corresponding operation on affine varieties $X \subset \overline{\mathbb{F}_q}^n$ and $Y \subset \overline{\mathbb{F}_q}^m$ is the direct product

$$X \times Y := \{(a, b) \mid a \in X, b \in Y\}.$$

The $(u|u+v)$ construction on linear codes $C_1 \subset \mathbb{F}_q^n$ and $C_2 \subset \mathbb{F}_q^n$ is the linear code

$$(C_1|C_1+C_2) := \{(u, u+v) \mid u \in C_1, v \in C_2\} \subset \mathbb{F}_q^{2n}$$

of length $2n$. For an affine variety $X \subset \overline{\mathbb{F}_q}^n$ and a morphism

$$g = (g_1, \dots, g_s) : \overline{\mathbb{F}_q}^n \longrightarrow \overline{\mathbb{F}_q}^s$$

with $g_1, \dots, g_s \in \mathbb{F}_q[x_1, \dots, x_n]$, the fibered product

$$X \times_{g(X)} \overline{\mathbb{F}_q}^n := \{(a, b) \in X \times \overline{\mathbb{F}_q}^n \mid g(a) = g(b)\}$$

is uniquely determined by the commutative diagram

$$\begin{array}{ccc} X & \xleftarrow{\text{pr}_1} & X \times_{g(X)} \overline{\mathbb{F}_q}^n \\ \downarrow g & & \downarrow \text{pr}_2 \\ g(X) & \xleftarrow{g} & \overline{\mathbb{F}_q}^n \end{array}$$

in which the parallel arrows correspond to maps with isomorphic fibres. Recall that an affine variety $Y = g^{-1}(0^s) \subset \overline{\mathbb{F}_q}^n$ with $I(Y, \overline{\mathbb{F}_q}) = \langle g_1, \dots, g_s \rangle_{\overline{\mathbb{F}_q}}$ is a complete intersection if $\dim Y = n - s$.

Proposition 20. (i) Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over \mathbb{F}_q and

$$\begin{aligned} \varphi_{n+1} : \overline{\mathbb{F}_q}^n &\longrightarrow \overline{\mathbb{F}_q}^{n+1}, \\ \varphi_{n+1}(x_1, \dots, x_n) &= \left(x_1, \dots, x_n, -\sum_{i=1}^n x_i \right) \quad \text{for } \forall (x_1, \dots, x_n) \in \overline{\mathbb{F}_q}^n \end{aligned}$$

be the extending map. Then the extension

$$\varphi_{n+1} T_a(X, \mathbb{F}_{q^{\delta(a)}}) = T_{\varphi_{n+1}(a)}(\varphi_{n+1}(X), \mathbb{F}_{q^{\delta(a)}}) \quad \text{for } \forall a \in X^{\text{smooth}} \quad (12)$$

of a Zariski tangent space to X is a Zariski tangent space to the extension $\varphi_{n+1}(X)$ of X .

(ii) Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ and $Y/\mathbb{F}_q \subseteq \overline{\mathbb{F}_q}^n$ be irreducible affine varieties, defined over \mathbb{F}_q . Then the direct sum

$$T_a(X, \mathbb{F}_{q^{\delta(a,b)}}) \oplus T_b(Y, \mathbb{F}_{q^{\delta(a,b)}}) = T_{(a,b)}(X \times Y, \mathbb{F}_{q^{\delta(a,b)}}) \quad \text{at } \forall (a, b) \in X^{\text{smooth}} \times Y^{\text{smooth}} \quad (13)$$

of tangent spaces to X and Y is a tangent space to $X \times Y$.

(iii) Let $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ be an irreducible affine variety, defined over \mathbb{F}_q and $g = (g_1, \dots, g_s) : \overline{\mathbb{F}_q}^n \rightarrow \overline{\mathbb{F}_q}^s$ with $g_1, \dots, g_s \in \mathbb{F}_q[x_1, \dots, x_n]$ be such a morphism that the fibre $Y_a := g^{-1}(a)/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$ through $a \in X^{\text{smooth}}$ is an irreducible complete intersection, containing a in its smooth locus. Then the $(u|u+v)$ construction

$$\left(T_a(X, \mathbb{F}_{q^{\delta(a)}}) \mid T_a(X, \mathbb{F}_{q^{\delta(a)}}) + T_a(Y_a, \mathbb{F}_{q^{\delta(a)}}) \right) = T_{(a,a)}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}) \quad (14)$$

of Zariski tangent spaces to X and Y_a is the tangent space to the fibered product $X \times_{g(X)} \overline{\mathbb{F}_q}^n$ at (a, a) .

Proof. (i) According to the inclusion $I(X, \overline{\mathbb{F}_q}) \subset I(\varphi_{n+1}(X), \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n, x_{n+1}]$ of the absolute ideals and $x_1 + \dots + x_n + x_{n+1} \in I(\varphi_{n+1}(X), \overline{\mathbb{F}_q})$, the Zariski tangent space $T_{\varphi_{n+1}(a)}(\varphi_{n+1}(X), \mathbb{F}_{q^{\delta(a)}})$ to $\varphi_{n+1}(X)$ at $\varphi_{n+1}(a) \in \varphi_{n+1}(X)$ is contained in the extension

$$\varphi_{n+1}T_a(X, \mathbb{F}_{q^{\delta(a)}}) := \left\{ \left(v, -\sum_{i=1}^n v_i \right) \in \mathbb{F}_{q^{\delta(a)}}^{n+1} \mid v \in T_a(X, \mathbb{F}_{q^{\delta(a)}}) \right\}$$

of $T_a(X, \mathbb{F}_{q^{\delta(a)}})$. If $a \in X^{\text{smooth}}$ then

$$\dim_{\mathbb{F}_{q^{\delta(a)}}} \varphi_{n+1}T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim X.$$

On the other hand, the biregular morphism $\varphi_{n+1} : X \rightarrow \varphi_{n+1}(X)$ has image $\varphi_{n+1}(X)$ of $\dim \varphi_{n+1}(X) = \dim X$, so that

$$\begin{aligned} \dim X = \dim \varphi_{n+1}(X) &\leq \dim T_{\varphi_{n+1}(a)}(\varphi_{n+1}(X), \mathbb{F}_{q^{\delta(a)}}) \leq \\ &= \dim_{\mathbb{F}_{q^{\delta(a)}}} \varphi_{n+1}T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim X \end{aligned}$$

and there follows (12) at all $a \in X^{\text{smooth}}$.

(ii) By $I(X, \overline{\mathbb{F}_q}) \subseteq I(X \times Y, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n, y_1, \dots, y_m]$ and $I(Y, \overline{\mathbb{F}_q}) \triangleleft I(X \times Y, \overline{\mathbb{F}_q})$ one has

$$\begin{aligned} T_{(a,b)}(X \times Y, \mathbb{F}_{q^{\delta(a,b)}}) &\subseteq T_a(X, \mathbb{F}_{q^{\delta(a,b)}}) \times T_b(Y, \mathbb{F}_{q^{\delta(a,b)}}) \simeq \\ &= T_a(X, \mathbb{F}_{q^{\delta(a,b)}}) \oplus T_b(Y, \mathbb{F}_{q^{\delta(a,b)}}). \end{aligned}$$

Note that $\dim(X \times Y) = \dim X + \dim Y$. If $a \in X^{\text{smooth}}$ and $b \in Y^{\text{smooth}}$ then

$$\begin{aligned} \dim X + \dim Y = \dim(X \times Y) &\leq \dim T_{(a,b)}(X \times Y, \mathbb{F}_{q^{\delta(a,b)}}) \leq \\ &= \dim T_a(X, \mathbb{F}_{q^{\delta(a,b)}}) \oplus \dim T_b(Y, \mathbb{F}_{q^{\delta(a,b)}}) = \dim X + \dim Y, \end{aligned}$$

whereas (13).

(iii) The inclusions $I(X, \overline{\mathbb{F}_q}) \subseteq I(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \overline{\mathbb{F}_q}) \triangleleft \overline{\mathbb{F}_q}[x_1, \dots, x_n, y_1, \dots, y_n]$ and $g_1(y) - g_1(x), \dots, g_s(y) - g_s(x) \in I(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \overline{\mathbb{F}_q})$ require the Zariski tangent space

$T_{(a,b)}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a,b)}})$ to be contained in the $\mathbb{F}_{q^{\delta(a,b)}}$ -linear code $C_{(a,b)}$ of length $2n$ with parity check matrix

$$H_{(a,b)} = \begin{pmatrix} \frac{\partial f}{\partial x}(a) & 0 \\ -\frac{\partial g}{\partial x}(a) & \frac{\partial g}{\partial y}(b) \end{pmatrix}.$$

Bearing in mind that $\frac{\partial g}{\partial y}(b)$ is the parity check matrix of $T_b(Y_a, \mathbb{F}_{q^m})$ for all $m \in \mathbb{N}$ with $\mathbb{F}_{q^m} \ni b$, one concludes that

$$C_{(a,a)} = (T_a(X, \mathbb{F}_{q^{\delta(a)}}) \mid T_a(X, \mathbb{F}_{q^{\delta(a)}}) + T_a(Y_a, \mathbb{F}_{q^{\delta(a)}}))$$

(cf.[8]). According to $a \in X^{\text{smooth}} \cap Y_a^{\text{smooth}}$, one has

$$\dim T_a(X, \mathbb{F}_{q^{\delta(a)}}) = \dim X, \quad \dim T_a(Y_a, \mathbb{F}_{q^{\delta(a)}}) = \dim Y_a = n - s \quad \text{and}$$

$$\dim C_{a \times a} = \dim X + n - s.$$

On the other hand, the fibered product $X \times_{g(X)} \overline{\mathbb{F}_q}^n$ is cut from $X \times \overline{\mathbb{F}_q}^n$ by s equations $g_i(x) = g_i(y)$, so that $\dim(X \times_{g(X)} \overline{\mathbb{F}_q}^n) \geq \dim X + n - s$. Now, the inclusion

$$T_{a \times a}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}) \subseteq C_{a \times a}$$

implies that

$$\begin{aligned} \dim X + n - s &\leq \dim(X \times_{g(X)} \overline{\mathbb{F}_q}^n) \leq \dim T_{a \times a}(X \times_{g(X)} \overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}) \leq \\ &\dim_{\mathbb{F}_{q^{\delta(a)}}} C_{a \times a} = \dim X + n - s \end{aligned}$$

and justifies (14). □

7 Families of Hamming isometries

Recall that the Hamming distance

$$d(a, b) := |\{1 \leq i \leq n \mid a_i \neq b_i\}|$$

between two words $a, b \in \mathbb{F}_q^n$ equals the number of their different components. A map $\mathcal{I} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is called a Hamming isometry if it preserves the Hamming distance, i.e., $d(\mathcal{I}a, \mathcal{I}b) = d(a, b)$ for $\forall a, b \in \mathbb{F}_q^n$. All Hamming isometries are bijective maps. More precisely, if we assume the existence of different $a, b \in \mathbb{F}_q^n$ with $\mathcal{I}a = \mathcal{I}b$ then $0 = d(\mathcal{I}a, \mathcal{I}b) = d(a, b)$ contradicts $a \neq b$.

7.1 Finite morphisms with isometric differentials

The present subsection provides a pattern for a construction of a global morphism $\psi : \overline{\mathbb{F}_q}^n \rightarrow \overline{\mathbb{F}_q}^n$ and a hypersurface $V(\psi_o) \subset \overline{\mathbb{F}_q}^n$, depending explicitly on ψ , such that the differentials of ψ restrict to linear Hamming isometries

$$(d\psi)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\psi(a)}(\psi(X), \mathbb{F}_{q^{\delta(a)}})$$

on the tangent codes to a generic affine variety $X \not\subset V(\psi_o)$ at a generic points $a \in X \setminus V(\psi_o)$.

Proposition 21. *For arbitrary polynomials $\psi_1, \dots, \psi_n \in \mathbb{F}_q[x_1, \dots, x_n]$ and an arbitrary permutation $\sigma \in \text{Sym}(n)$, let us consider the morphism*

$$\psi := (x_{\sigma(1)}\psi_{\sigma(1)}(x_1^p, \dots, x_n^p), \dots, x_{\sigma(n)}\psi_{\sigma(n)}(x_1^p, \dots, x_n^p)) : \overline{\mathbb{F}_q}^n \longrightarrow \overline{\mathbb{F}_q}^n$$

and the hypersurface $V(\psi_o) \subset \overline{\mathbb{F}_q}^n$ with equation

$$\psi_o(x_1, \dots, x_n) := \psi_1(x_1^p, \dots, x_n^p) \dots \psi_n(x_1^p, \dots, x_n^p),$$

where $p = \text{char}(\mathbb{F}_q)$ stands for the characteristic of the basic field \mathbb{F}_q . Then any irreducible affine variety $X \subset \overline{\mathbb{F}_q}^n$, which is not entirely contained in the hypersurface $V(\psi_o)$ has a non-empty Zariski open, Zariski dense subset

$$W := \left[X^{\text{smooth}} \cap \psi^{-1}(\psi(X)^{\text{smooth}}) \right] \setminus V(\psi_o),$$

such that the differentials of ψ restrict to $\mathbb{F}_{q^{\delta(a)}}$ -linear Hamming isometries

$$(d\psi)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\psi(a)}(\psi(X), \mathbb{F}_{q^{\delta(a)}})$$

at all the points $a \in W$.

Proof. It suffices to prove the proposition for the \mathbb{F}_q -morphism

$$\varphi := \sigma^{-1}\psi = (\varphi_1 = x_1\psi_1(x_1^p, \dots, x_n^p), \dots, \varphi_n = x_n\psi_n(x_1^p, \dots, x_n^p)) : X \longrightarrow \psi(X),$$

as far as the permutation $\sigma^{-1} \in \text{Sym}(n)$ coincides with its differentials at any point $a \in \overline{\mathbb{F}_q}^n$ and is a linear Hamming isometry. Let

$$\begin{aligned} \Phi_p : \mathbb{F}_q[x_1, \dots, x_n] &\longrightarrow \mathbb{F}_q[x_1, \dots, x_n], \\ \Phi_p(f(x_1, \dots, x_n)) &:= f(x_1^p, \dots, x_n^p) \end{aligned}$$

be the Frobenius automorphism of $\mathbb{F}_q[x_1, \dots, x_n]$ of degree $p = \text{char}\mathbb{F}_q$. The differential

$$(d\varphi)_a : T_a(\overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow T_{\varphi(a)}(\overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}})$$

of the morphism $\varphi := (x_1\psi_1(x_1^p, \dots, x_n^p), \dots, x_n\psi_n(x_1^p, \dots, x_n^p))$ has matrix

$$\frac{\partial(\psi_1, \dots, \psi_n)}{\partial(x_1, \dots, x_n)}(a) = \begin{pmatrix} \psi_1(\Phi_p(a)) & 0 & \dots & 0 \\ 0 & \psi_2(\Phi_p(a)) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \psi_n(\Phi_p(a)) \end{pmatrix}$$

with respect to the basis $\left(\frac{\partial}{\partial x_j}\right)_a$, $1 \leq i \leq n$ of $T_a(\overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}})$. Note that at any point $a \in (X \setminus V(\psi_o))$ the differential $(d\varphi)_a : T_a(\overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}}) \rightarrow T_{\varphi(a)}(\overline{\mathbb{F}_q}^n, \mathbb{F}_{q^{\delta(a)}})$ is an $\mathbb{F}_{q^{\delta(a)}}$ -linear Hamming isometry and restricts to an $\mathbb{F}_{q^{\delta(a)}}$ -linear Hamming isometry

$$(d\varphi)_a : T_a(X, \mathbb{F}_{q^{\delta(a)}}) \longrightarrow (d\varphi)_a T_a(X, \mathbb{F}_{q^{\delta(a)}}) \subseteq T_{\varphi(a)}(\varphi(X), \mathbb{F}_{q^{\delta(a)}})$$

onto its image. We claim that $W \neq \emptyset$ is a non-empty Zariski open subset. Due to the irreducibility of X it suffices to note that $X^{\text{smooth}} \neq \emptyset$, $X \setminus V(\psi_o) \neq \emptyset$ and the non-empty Zariski open subset $\varphi(X)^{\text{smooth}} \subseteq \varphi(X)$ pulls back to a non-empty Zariski open subset $X \cap \varphi^{-1}(\varphi(X)^{\text{smooth}}) \neq \emptyset$ of X . \square

7.2 Interpolation of linear Hamming isometries by a morphism

The next proposition realizes the members $\mathcal{I}(a) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ of an arbitrary family $\mathcal{I} \rightarrow S$ of \mathbb{F}_q -linear Hamming isometries over $S \subseteq \mathbb{F}_q^n$ by the differentials $(d\varphi)_a = \mathcal{I}(a)$ of an appropriate \mathbb{F}_q -morphism $\varphi : \overline{\mathbb{F}_q}^n \rightarrow \overline{\mathbb{F}_q}^n$.

Proposition 22. *Let $\mathcal{I} \rightarrow S$ be a family of \mathbb{F}_q -linear Hamming isometries $\mathcal{I}(a) \in \text{GL}(n, \mathbb{F}_q)$, $\mathcal{I}(a) : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, parameterized by a subset $S \subseteq \mathbb{F}_q^n$. Then there exists an \mathbb{F}_q -morphism $\varphi = (\varphi_1, \dots, \varphi_n) : \overline{\mathbb{F}_q}^n \rightarrow \overline{\mathbb{F}_q}^n$, whose differentials $(d\varphi)_a = \mathcal{I}(a)$ at $\forall a \in S$ coincide with the given isometries.*

Proof. Let us consider the polynomials

$$\varphi_i(x_1, \dots, x_n) := \sum_{b \in \Phi_p(S)} \left[\sum_{j=1}^n \mathcal{I}(\Phi_p^{-1}(b))_{ij} (x_j - x_j^q) \right] L_{\mathbb{F}_q}^{b_1}(x_1^p) \dots L_{\mathbb{F}_q}^{b_n}(x_n^p)$$

for $1 \leq i \leq n$, where

$$\begin{aligned} \Phi_p : \overline{\mathbb{F}_q}^n &\longrightarrow \overline{\mathbb{F}_q}^n, \\ \Phi_p(a_1, \dots, a_n) &= (a_1^p, \dots, a_n^p) \quad \text{for } \forall a = (a_1, \dots, a_n) \in \overline{\mathbb{F}_q}^n \end{aligned}$$

is the Frobenius automorphism of degree $p = \text{char} \mathbb{F}_q$ and

$$L_{\mathbb{F}_q}^\beta(t) := \prod_{\alpha \in \mathbb{F}_q \setminus \{\beta\}} \frac{t - \alpha}{\beta - \alpha} = \begin{cases} -t^{q-1} + 1 & \text{for } \beta = 0, \\ -t^{q-1} - \sum_{s=1}^{q-2} \beta^{-s} t^s & \text{for } \beta \in \mathbb{F}_q^* \end{cases}$$

stand for the Lagrange basis polynomials, used in Proposition 5. Straightforwardly,

$$\frac{\partial \varphi_i}{\partial x_j} = \sum_{b \in \Phi_p(S)} \mathcal{I}(\Phi_p^{-1}(b))_{ij} L_{\mathbb{F}_q}^{b_1}(x_1^p) \dots L_{\mathbb{F}_q}^{b_n}(x_n^p)$$

for $\forall 1 \leq i, j \leq n$, whereas

$$\frac{\partial \varphi_i}{\partial x_j}(a) = \mathcal{I}(a)_{ij} \quad \text{at } \forall a \in S \subseteq \mathbb{F}_q^n.$$

Therefore $\mathcal{I}(a) \in \mathrm{GL}(n, \mathbb{F}_q)$ is the matrix of the differential

$$(d\varphi)_a : T_a(\overline{\mathbb{F}_q}^n, \mathbb{F}_q) \longrightarrow T_{\varphi(a)}(\overline{\mathbb{F}_q}^n, \mathbb{F}_q)$$

with respect to the basis $\left(\frac{\partial}{\partial x_j}\right)_a$, $1 \leq j \leq n$ of $T_a(\overline{\mathbb{F}_q}^n, \mathbb{F}_q)$. □

Note that the Frobenius automorphism

$$\Phi_q : \overline{\mathbb{F}_q}^n \longrightarrow \overline{\mathbb{F}_q}^n,$$

$$\Phi_q(x_1, \dots, x_n) = (x_1^q, \dots, x_n^q)$$

restricts to a bijective morphism $\Phi_q : X \rightarrow X$ on any affine variety $X/\mathbb{F}_q \subset \overline{\mathbb{F}_q}^n$, defined over \mathbb{F}_q . The morphism Φ_q is not an isomorphism, as far as its inverse map $\Phi_q^{-1} : X \rightarrow X$ is not a morphism. For any $m \in \mathbb{N}$ there arises a bijective map $\Phi_q : X(\mathbb{F}_{q^m}) \rightarrow X(\mathbb{F}_{q^m})$ of the set $X(\mathbb{F}_{q^m})$ of the \mathbb{F}_{q^m} -rational points of X . In particular, the Frobenius automorphism $\Phi_q = \mathrm{Id} : X(\mathbb{F}_q) \rightarrow X(\mathbb{F}_q)$ restricts to the identity on the \mathbb{F}_q -rational points of X . One can view

$$\Phi_q : T(X, \mathbb{F}_{q^m}) \longrightarrow T(X, \mathbb{F}_{q^m})$$

as a non-linear Hamming isometry of the Zariski tangent bundles $T(X, \mathbb{F}_{q^m})$ for any $m \in \mathbb{N}$. Note that $\Phi_q : T_a(X, \mathbb{F}_{q^m}) \rightarrow T_{\Phi_q(a)}(X, \mathbb{F}_{q^m})$ interchanges the fibres over $a \in X(\mathbb{F}_{q^m}) \setminus X(\mathbb{F}_q)$ and acts on the fibres $\Phi_q : T_a(X, \mathbb{F}_{q^m}) \rightarrow T_a(X, \mathbb{F}_{q^m})$ over $a \in X(\mathbb{F}_q)$.

References

- [1] C. W. Ayoub, The decomposition theorem for ideals in polynomial rings over a domain, *Journal of Algebra*, **76** (1982), 99–110.
- [2] M. C. Beltrametti, E. Carletti, D. Gallarati, G. M. Bragadin, *Lectures on Curves, Surfaces and Projective Varieties (A Classical View of Algebraic Geometry)* European Mathematical Society Textbooks, Zürich, 2009.
- [3] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer, 1997.
- [4] S. Dodunekov and I. Landgev, Near MDS-codes, *Journal of Geometry*, **54** (1995), 30–43.
- [5] D. Eisebud, C. Huneke, W. Vascocelos, Direct methods for primary decomposition, *Inventiones Mathematicae*, **110** (1992), 207–235.
- [6] P Gianni, B. Trager, G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, *Journal of Symbolic Computation*, **6** (1988), 149–167.

- [7] J. Harris, *Algebraic Geometry - A First Course*, Graduate Texts in Mathematics, Springer, 1992.
- [8] W. C. Huffman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.
- [9] A. Kasparian, I. Marinov, Goppa families of linear codes, Preprint.
- [10] R. Matsumoto, Computing the radical of an ideal in positive characteristic, *Journal of Symbolic Computation*, **32** (2001), 263–271.
- [11] K. O’Grady, *A First Course in Algebraic Geometry*, 2012.
- [12] R. Pellikaan On the efficient decoding of algebraic-geometric codes, *Eurocode 92* (P. Camion, P. Charpin and S. Harari eds.) Udine, CISM Courses and Lectures **339**, Springer, Wien, 1993, 231–253.
- [13] G. Pfister, A. Sadiq, S. Steidel, An algorithm for primary decomposition in polynomial rings over the integers, *Central European Journal of Mathematics*, **9** (2011), 897–904.
- [14] M. Reid, *Undergraduate Algebraic Geometry*, London Mathematical Society Student Texts, 1989.
- [15] A. Sausse, A new approach to primary decomposition, *Journal of Symbolic Computation*, **11** (1996), 1–15.
- [16] I. R. Shafarevich, *Basic Algebraic Geometry*, v.1, 2, Moscow, 1988.
- [17] M. A. Tsfasman, S. G. Vlădut, T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.
- [18] J. Wu, On the algebraic variety decomposition, *Systems Science and Mathematical Sciences*, **9** (1996), 120–127.